ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова праця
на правах рукопису

ЯЦИНА ЮЛІЯ ОЛЕКСАНДРІВНА

УДК [32:343.352]:004.021:303.093.6(477)

ДИСЕРТАЦІЯ

ІННОВАЦІЙНІ АНАЛІТИКО-СТАТИСТИЧНІ ТЕХНОЛОГІЇ ПОПЕРЕДЖЕННЯ КОРУПЦІЇ В ДЕРЖАВІ

За спеціальністю 052 – Політологія
Галузь знань 05 – Соціальні та поведінкові науки

Подається на здобуття наукового ступеня доктора філософії

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

_____ Ю.О. Яцина

Науковий керівник:
Цокур Євген Георгійович,
доктор політичних наук, професор

Запоріжжя – 2025

АНОТАЦІЯ

Яцина Ю.О. Інноваційні аналітико-статистичні технології попередження корупції в державі. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю «052 – Політологія». Запорізький національний університет, Запоріжжя, 2025.

Умови системної турбулентності, в яких опинилася публічна влада в Україні, загострюють потребу в переосмисленні стратегій боротьби з корупцією не як суто правового процесу, а як складного феномену, що потребує залучення інструментів сучасного аналітичного мислення. Цифровізація управління відкрила нові горизонти моніторингу та попередження зловживань, однак водночас актуалізувала проблему інституційної адаптації. Відтак виникає потреба в комплексному аналізі інноваційних аналітико-статистичних технологій, здатних не лише зафіксувати наявні корупційні прояви, але й передбачити, попередити та трансформувати саму логіку їхнього виникнення.

Дисертація містить огляд ключових наукових напрацювань у сфері впровадження інноваційних аналітико-статистичних технологій як інструменту автоматизації процесів попередження корупції в державі. Проведене дослідження показало, що феномен корупції не зводиться до правопорушення чи економічного злочину, а являє собою багатовимірне соціальне, політичне, психологічне й культурне утворення. У дисертації корупція розглядається як правова девіація, соціально-політичний інститут, культурно-психологічний феномен і набір групових стратегій, що водночас є наслідком і індикатором деформації механізмів врядування. Попередження корупції визначено як систему цілеспрямованих дій, методів, процедур або технологічних рішень, спрямованих на виявлення, нейтралізацію або трансформацію соціальних, управлінських, інституційних і психологічних факторів, які потенційно сприяють корупційній поведінці, ще до того, як така поведінка набуде форми

фактичного правопорушення. Інноваційні аналітико-статистичні технології у широкому сенсі розглянуто як сукупність методів математичного аналізу, машинного навчання, аналізу даних і цифрової моделі прийняття рішень.

Охарактеризовано основні методологічні засади дослідження інноваційних аналітико-статистичних технологій попередження корупції в державі та обґрунтовано основні наукові принципи та методи дослідження.

Здійснено аналіз сучасних підходів до розуміння сутності держави, що є не лише джерелом ризиків і середовищем формування корупційних практик, але й центральним суб'єктом їх системного попередження. Її інституційна багатовимірність, що поєднує публічну владу, корпоративні структури та неформальні механізми впливу, створює як сприятливе середовище для зловживань, так і потенціал для трансформацій. Визначено, що запорукою дієвих змін виступає зміна логіки функціонування державних інститутів: від політико-бюрократичної замкнутості – до відкритої, цифрово-підзвітної моделі, у якій пріоритет надається не лише контролю за порушеннями, а й системній діагностиці їх передумов.

Ретроспективний аналіз розвитку інформаційних технологій визначив, що аналітико-статистичні технології слід розуміти як спеціальні інформаційні технології, що формують інформаційні системи на основі великих даних, алгоритмів штучного інтелекту, машинного навчання та засобів візуалізації. Вони орієнтовані на прогнозування ризиків, підтримку прийняття рішень і створення експертних систем. Визначено, що інноваційна сутність аналітико-статистичних підходів проявляється у їхній здатності перетворювати інформаційний ресурс на антикорупційний інструмент на рівні держави. У цьому контексті аналітико-статистичні технології виступають не як нейтральний технічний інструмент, а як ядро цифрової трансформації управління. Їх функція полягає не лише у скороченні адміністративних витрат чи мінімізації контакту з чиновником, а й у формуванні нової архітектури державної взаємодії – орієнтованої на дані, прозору, сервісну. Однак технологічна ефективність можлива лише за умови побудови нормативно й організаційно інтегрованої

цифрової інфраструктури. Успішна антикорупційна політика повинна мислитися не як сукупність розрізнених ІТ-ініціатив, а як єдина цифрова екосистема, що передбачає зміну культури прийняття рішень на всіх рівнях управління.

Для розуміння особливостей застосування спеціальних інформаційних технологій в антикорупційній діяльності, здійснено аналіз існуючих підходів до виявлення корупційних загроз. Визначено, що особливу складність становить боротьба з внутрішніми корупційними загрозами, які не залишають цифрових слідів у формальному розумінні, але проявляються у поведінкових відхиленнях, маніпуляціях із правом доступу до даних та зловживаннях на рівні службових повноважень. У таких випадках ключову роль відіграють алгоритми поведінкового моніторингу, виявлення аномалій, профілювання та кластеризації, що вимагають не лише глибоких технічних знань, а й високої аналітичної культури серед працівників державних інституцій. Лише поєднання технічних, організаційних та когнітивних підходів дозволяє реалізувати логіку попередження, а не реагування. І саме ця синергетика – цифрова, аналітична, інституційна – стає визначальною для переходу від декларативної антикорупційної політики до структурної доброчесності. Особливу увагу приділено системам, що поєднують принципи штучного інтелекту та відкритих даних, зокрема на базі платформ Prozorro, Dozorro, Opendatabot, YouControl. Висунуто тезу про те, що ефективність таких систем залежить не лише від технологічного забезпечення, але й від політичної волі та здатності органів влади інституціоналізувати принципи прозорості й підзвітності.

Здійснено огляд функціональних напрямків та технологічних платформ реалізації аналітико-статистичних систем попередження корупції в державному управлінні. Показано, що ефективність таких систем визначається їх здатністю автоматизувати рутинні інформаційні та управлінські процеси, зменшувати ймовірність людських помилок, а також забезпечувати високий рівень структурованості даних для подальшого аналізу. Обґрунтовано, що сучасні корпоративні системи (ERP, CRM, SCM, BI, DSS) не лише підвищують точність прийняття управлінських рішень, але й виступають каталізаторами прозорості,

особливо у сферах закупівель, кадрів, логістики. Окрему увагу приділено ролі систем штучного інтелекту й машинного навчання, що дозволяють переходити від виявлення до прогнозування корупційних ризиків.

Визначено, що впровадження інноваційних аналітико-статистичних технологій у сфері попередження корупції відбувається за двома стратегічними векторами: інституційно-нормативним «зверху вниз» та громадянсько-активістським «знизу вгору». У першому випадку використання технологій, зокрема штучного інтелекту, слугує інструментом реалізації державної політики, як це демонструє кейс системи Kalsada на Філіппінах. У другому – ініціативи громадянського суспільства, як-от український портал Dozorro, забезпечують незалежний моніторинг дій влади через аналіз відкритих даних. Встановлено, що інтеграція обох підходів формує більш стійку інституційну екосистему, в якій цифрові технології виконують не лише функцію контролю, а й підтримують процеси демократизації управління та зміцнення довіри до антикорупційної політики.

На підставі огляду наявних досліджень про досвід застосування аналітико-статистичних технологій, було визначено чотири напрями: вторинний аналіз даних, автоматизований аналіз текстів, методологічні розробки та експериментальні кейси. Перший напрям дозволяє виявити ключові макроекономічні й політичні індикатори корупції та формувати на їх основі прогнозні моделі. Другий – забезпечує напівавтоматизоване виявлення корупційних практик через вивчення змісту ЗМІ, судових рішень і аналітичних звітів. Методологічний напрямок зосереджений на створенні універсальних алгоритмів для виявлення аномалій і моделювання ризиків, зокрема в графових структурах або часових рядах. А експериментальні дослідження – зокрема в сфері охорони здоров’я, державних закупівлях та електоральному процесі – демонструють реальні способи застосування цих технологій для виявлення змов, картельних змов, а також статистичних аномалій, які свідчать про потенційні порушення.

Окрему увагу в дослідженні приділено авторським розробкам, створеним для підвищення ефективності роботи антикорупційних практиків і дослідників. Серед них – Python-скрипти для збору, стенографування та перекладу текстових даних, а також інструмент верифікації публічної інформації. Їх апробація здійснювалася під час навчальних і виробничих практик студентів Факультету соціології та управління Запорізького національного університету. Визначено, що подібні інструменти становлять собою приклад демократизації аналітичного ресурсу, коли сучасні технології стають доступними не лише великим інституціям, а й дослідникам і громадським активістам на місцевому рівні.

Проведений аналіз дозволив визначити ризики, пов’язані з надмірною технологізацією антикорупційної діяльності. Вказано, що самі по собі цифрові рішення не гарантують ефективності, якщо не супроводжуються політичною волею, правовими запобіжниками та суспільною підтримкою. Сценарний підхід дозволив змоделювати три потенційні вектори розвитку цифрової антикорупційної інфраструктури в Україні – песимістичний, реалістичний та оптимістичний. Показано, що лише комплексна інтеграція інновацій у політичну й управлінську культуру здатна трансформувати цифрові інструменти з формальних рішень на дієві механізми інституційної доброчесності.

Ключові слова: автоматизація, аналітика, антикорупційна діяльність, антикорупційна політика, віртуалізація держави, держава, інноваційні аналітико-статистичні технології, інноваційні технології, інновація, інформаційна загроза, інформаційний простір, інформаційні технології, інформація, корупція, криміналістика, машинне навчання, прозорість, попередження / протидія корупції, статистика, цифрові технології, цифровізація держави, штучний інтелект.

ABSTRACT

Yatsyna Y.O. Innovative analytical and statistical technologies for preventing corruption in the state. – *Qualification scientific work in the form of a manuscript.*

Dissertation for the degree of Doctor of Philosophy in the specialty «052 – Political Science». Zaporizhzhia National University, Zaporizhzhia, 2025.

The conditions of systemic turbulence currently facing public governance in Ukraine have intensified the need to reconceptualize anti-corruption strategies not merely as legal procedures, but as responses to a complex phenomenon that requires the engagement of advanced analytical thinking. The digitalization of public administration has opened new horizons for monitoring and preventing abuse, yet at the same time, it has highlighted the problem of institutional adaptation. This necessitates a comprehensive analysis of innovative analytical and statistical technologies capable not only of detecting existing manifestations of corruption, but also of predicting, preventing, and transforming the very logic of their emergence.

The dissertation provides an overview of key scholarly developments in the field of implementing innovative analytical and statistical technologies as tools for automating processes aimed at preventing corruption in the state. The study demonstrates that corruption cannot be reduced to a legal infraction or economic crime; rather, it represents a multidimensional socio-political, psychological, and cultural construct. In the dissertation, corruption is conceptualized as a legal deviance, a socio-political institution, a cultural-psychological phenomenon, and a set of group strategies that simultaneously constitute both the outcome and indicator of governance failures. Corruption prevention is defined as a system of targeted actions, methods, procedures, or technological solutions aimed at identifying, neutralizing, or transforming the social, governmental, institutional, and psychological factors that may contribute to corrupt behavior before such behavior materializes as a legal offense. Innovative analytical and statistical technologies are understood in a broad sense as an array of methods from

mathematical analysis, machine learning, data analytics, and algorithmic decision-making models.

The dissertation characterizes the main methodological foundations for studying innovative analytical and statistical technologies in the context of corruption prevention in the state and substantiates the key scientific principles and methods employed throughout the research.

An analysis of contemporary approaches to understanding the nature of the state reveals that it is not only a source of risk and an environment for the formation of corrupt practices, but also the central actor in their systematic prevention. The state's institutional multidimensionality – encompassing public authority, corporate structures, and informal mechanisms of influence – simultaneously fosters opportunities for abuse and contains the potential for structural transformation. The research identifies that effective change depends on a fundamental shift in the logic of institutional functioning: from a closed, bureaucratic-political model to an open, digitally accountable framework, where priority is given not only to the control of violations, but to the systemic diagnosis of their underlying causes.

A retrospective analysis of the development of information technologies demonstrates that analytical and statistical technologies should be understood as specialized information systems based on big data, artificial intelligence algorithms, machine learning methods, and visualization tools. These technologies are aimed at risk forecasting, decision-making support, and the creation of expert systems. The study finds that the innovative nature of analytical and statistical approaches is manifested in their capacity to transform informational resources into anti-corruption instruments at the level of state governance. In this context, analytical and statistical technologies are not merely neutral technical tools – they form the core of the digital transformation of public administration. Their function extends beyond reducing administrative costs or minimizing direct contact between citizens and officials; they are instrumental in constructing a new architecture of state interaction – data-driven, transparent, and service-oriented. However, technological efficacy can only be achieved through the development of a normative and organizationally integrated

digital infrastructure. Successful anti-corruption policy should not be perceived as a collection of isolated IT initiatives, but rather as a coherent digital ecosystem that redefines the culture of decision-making at all levels of governance.

To understand the specific application of specialized information technologies in anti-corruption efforts, the study analyzes existing approaches to identifying corruption-related threats. It is established that particular challenges arise in addressing internal corruption threats, which often leave no formal digital traces but manifest through behavioral deviations, manipulation of data access rights, and abuses of administrative authority. In such cases, behavioral monitoring algorithms, anomaly detection, profiling, and clustering techniques become crucial. These require not only advanced technical expertise but also a high level of analytical culture among public officials. Only through the integration of technical, organizational, and cognitive approaches can a shift from reactive measures to a logic of prevention be effectively achieved. This synergy – digital, analytical, and institutional – proves essential for transitioning from declarative anti-corruption policies to structurally embedded integrity. Special attention is given to systems that combine artificial intelligence with open data infrastructures, notably platforms such as Prozorro, Dozorro, Opendatabot, or YouControl. The study posits that the effectiveness of such systems depends not only on their technological capabilities but also on the political will and institutional readiness of government agencies to embed principles of transparency and accountability.

A review of the functional domains and technological platforms for implementing analytical and statistical systems of corruption prevention in public administration reveals that their effectiveness is closely linked to their capacity to automate routine informational and managerial processes, reduce human error, and provide a high degree of data structuring for further analysis. The research substantiates that modern enterprise-level systems – ERP, CRM, SCM, BI, DSS – are not only instrumental in enhancing decision-making accuracy but also act as catalysts of institutional transparency, particularly in procurement, human resources, and logistics. Particular emphasis is placed on the role of artificial intelligence and machine learning

systems, which enable the transition from post-factum detection to proactive forecasting of corruption risks.

It has been determined that the implementation of innovative analytical and statistical technologies in the field of corruption prevention follows two strategic trajectories: the top-down institutional and regulatory approach, and the bottom-up civic-activist approach. In the first case, technologies – particularly artificial intelligence – serve as tools for executing state policy, as illustrated by the Kalsada system in the Philippines. In the second, civil society initiatives, such as the Ukrainian platform Dozorro, enable independent oversight of government actions through the analysis of open data. The integration of both approaches creates a more resilient institutional ecosystem in which digital technologies not only perform a control function but also support the democratization of governance and the strengthening of public trust in anti-corruption policy.

Based on a review of existing studies concerning the application of analytical and statistical technologies, four key directions have been identified: secondary data analysis, automated text analysis, methodological development, and experimental case studies. The first direction enables the identification of macroeconomic and political indicators of corruption and the construction of predictive models based on them. The second facilitates semi-automated detection of corrupt practices through the analysis of media content, judicial decisions, and analytical reports. The methodological direction focuses on the creation of universal algorithms for anomaly detection and risk modeling, particularly in graph structures or time series. Experimental research – especially in healthcare, public procurement, and electoral processes – demonstrates real-world applications of these technologies in uncovering collusion, cartel behavior, and statistical anomalies that may indicate potential violations.

Particular attention in the study is given to the author’s original developments aimed at enhancing the effectiveness of anti-corruption practitioners and researchers. Among these are Python scripts designed for the collection, transcription, and translation of textual data, as well as a tool for verifying public information. These tools were piloted during the academic and field internships of students from Social

Science and Public Administration faculty at Zaporizhzhia National University. It is emphasized that such instruments represent an example of the democratization of analytical resources – making modern technologies accessible not only to large institutions but also to researchers and civic activists at the local level.

The analysis conducted also made it possible to identify the risks associated with the excessive technologization of anti-corruption activities. It is noted that digital solutions alone do not ensure effectiveness unless supported by political will, legal safeguards, and public engagement. The use of scenario modeling allowed for the identification of three potential development pathways for Ukraine's digital anti-corruption infrastructure: pessimistic, realistic, and optimistic. The findings suggest that only the comprehensive integration of innovation into political and administrative culture can transform digital tools from formal solutions into effective mechanisms of institutional integrity.

Keywords: artificial intelligence, automation, analytics, anti-corruption activity, anti-corruption policy, virtualization of state, state, innovative analytical and statistical technologies, innovation, information, information threat, information space, information technologies, corruption, forensics, machine learning, transparency, corruption prevention / counteraction, statistics, digital technologies, digitalization of state.

СПИСОК НАУКОВИХ ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті в наукових фахових виданнях, включених до переліку наукових фахових видань України:

1. Яцина, Ю. (2023). Уточнення змісту основних понять проблеми інноваційних аналітико-статистичних технологій як інструменту протидії корупції. *Філософія та політологія в контексті сучасної культури*, 15(1), 85-95. DOI: https://doi.org/10.15421/352311

2. Яцина Ю.О. (2023). Напрямки впровадження інноваційних аналітико-статистичних технологій як інструменту протидії корупції в державі. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право,* 1(57), 164-174. DOI: https://doi.org/10.20535/2308-5053.2023.1(57).280822

3. Яцина, Ю.О. (2023). Особливості застосування інноваційних аналітико-статистичних технологій в інформаційних системах з моніторингу та виявлення корупції. *Актуальні проблеми філософії та соціології*, 40, 206-213. DOI: https://doi.org/10.32782/apfs.v040.2023.35

4. Яцина, Ю.О. (2023). Інноваційні аналітико-статистичні технології як інструмент моніторингу та протидії корупції. *Епістемологічні дослідження в філософії, соціальних і політичних науках*, 6(1), 145-156. DOI: https://doi.org/10.15421/342319

5. Kudinov, I., Sičáková-Beblavá, E., & Yatsyna, Y. (2017). Actors of Political Life in Ukraine: Social Portrait of Contemporary Power Elite. *Нова парадигма* : *[журнал наукових праць]* / голов. ред. В. П. Бех. ; Нац. пед. ун-т імені М.П. Драгоманова ; творче об’єднання «Нова парадигма». Київ : Вид-во НПУ імені М.П. Драгоманова, 133, 95-111. URL: https://www.novaparadigma.npu.edu.ua/index.php/novaparadigma/article/view/15/13

6. Кудінов, І., Сичакова-Беблава, Е., & Яцина, Ю. (2017). Суб'єкти політичного життя України: соціальний портрет сучасної правлячої еліти. *Культурологічний вісник: Науково-теоретичний щорічник Нижньої*

Наддніпрянщини / Гол. ред. М.А. Лепський; Запорізький національний університет. Запоріжжя : КСК-Альянс, 38(2), 81-92. DOI: https://doi.org/10.26661/2413-2284-2017-2-38-09

7. Yatsyna, Y., & Kudinov, I. (2017). Corruption in the Higher Educational System of Ukraine. *Нова парадигма : [журнал наукових праць]* / голов. ред. В. П. Бех. ; Нац. пед. ун-т імені М. П. Драгоманова ; творче об'єднання «Нова парадигма». Київ : Вид-во НПУ імені М.П. Драгоманова, 132, 44-52. URL: https://www.novaparadigma.npu.edu.ua/index.php/novaparadigma/article/view/19/35

Статті у періодичних наукових виданнях інших держав, які входять до Організації економічного співробітництва та розвитку та/або Європейського Союзу, з наукового напряму, за яким підготовлено дисертацію здобувача:

1. Yatsyna, Y., & Kudinov, I. (2023). Directions for the implementation of innovative analytical and statistical technologies as a tool for corruption counteraction. *Laisvalaikio Tyrimai*, 2(22), 17-29. DOI: https://doi.org/10.33607/elt.v2i22.1440

2. Yatsyna, Y., & Kudinov, I. (2023). Innovative analytical and statistical technologies in election forensics. *Regional Formation and Development Studies*, 2(40), 28-42. DOI: https://doi.org/10.15181/rfds.v40i2.2528

Статті в наукових фахових виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus

1. Yatsyna, Y., & Kudinov, I. (2023). Innovative analytical and statistical technology as a corruption counteraction tool: conceptual analysis. *Amazonia Investiga*, 12(67), 78-86. DOI: https://doi.org/10.34069/AI/2023.67.07.7

2. Lepska, N., Lepskyi, M., Yatsyna, Y., & Kudinov, I. (2021). The isolationist pathology of sovereignism (three historical cases for analysis). *WISDOM*, 19(3), 151-162. DOI: https://doi.org/10.24234/wisdom.v19i3.487.

Розділ колективної монографії:

1. Кудінов, І.О., & Яцина, Ю.О. (2024). Інноваційні технології автоматизації збору та обробки даних у дослідженні політичних процесів та ситуацій. *Технології державотворення в умовах сучасної політичної дійсності : колективна монографія* / Д. Ю. Арабаджиєв, О. М. Вагіна, Н. В. Горло, О. М. Кіндратець, І. О. Кудінов, Н. В. Лепська, Ю. Г. Мальована, А. О. Руднєва, Т. І. Сергієнко, Л. С. Хорішко, Є. Г. Цокур, Ю. О. Яцина ; за заг. ред. Н. В. Горло. Запоріжжя : Запорізький національний університет, 266-287. URL: https://files.znu.edu.ua/files/ZNU_Monographs/0060900.pdf

Матеріали наукових конференцій:

1. Яцина, Ю. (2024). *Міжнародний досвід застосування дисциплінарної відповідальності за корупційні правопорушення*. Інформаційне суспільство і Природа: вектори взаємовпливу : збірка матеріалів VIII Міжнародної науково-практичної конференції (м. Кривий Ріг, 21-22 листопада 2024 р.) / за заг. ред. д.соц.н., проф. Л. Калашнікової. Київ : Вид-во «Каравела», 105-110.

2. Кудінов, І., & Яцина, Ю. (2024). *Популізм як феномен політичного життя.* Філософія і культура в антропологічних вимірах сучасності : зб. тез доп. XIII наук. конф. з нагоди Всесвіт. Дня Філософії (UNESCO), 22–23 листоп. 2024 р. / М-во освіти і науки України, Укр. держ. ун-т науки і технологій, каф. Філософії та українознавства, КЗВО «Дніпров. акад. музики» ДОР, Ін-т світ. культури, КЗВО «Дніпров. акад. неперерв. освіти» ДОР, кафедра Філософії. Дніпро : УДУНТ. URL: https://conf-ampr.ust.edu.ua/AMPRX13/paper/view/32235/18899

3. Yatsyna, Y. (2024). *International experience of disciplinary responsibility for corruption offenses*. Матеріали IX Міжнародної науково-практичної конференції студентів, аспірантів і молодих учених «Технології відновлення країни в умовах глобальних ризиків та невизначеностей» (29 листопада 2024 року, м. Запоріжжя). Запоріжжя : ЦНСД, 67-70. URL: https://socforecast.org.ua/wp-content/uploads/soctech2024.pdf

4. Yatsyna, Y., & Kudinov, I. (2023). *Innovative analytical and statistical technologies as a tool for fraud and corruption detection*. The 19th International conference “Social Innovations for Sustainable Regional Development”: Klaipėda, Lithuania, April 27-28, 2023. Abstracts of reports. Klaipėda: Klaipėda University, 51-54. URL: https://shmf.ku.lt/uploads/documents/files/social_conference_2023_for_publishing(2).pdf

5. Yatsyna, Y., & Kudinov, I. (2023). *Corruption as a Type of Fraud*. Матеріали XIII Міжнародної наукової конференції «Соціальне прогнозування та проєктування майбутнього: перемога, мир та відновлення у післявоєнній Україні» (28 квітня 2023 року, м. Запоріжжя). Запоріжжя : ЦНСД, 86-89. URL: https://socforecast.org.ua/wp-content/uploads/socforecast2023.pdf

6. Yatsyna, Y., & Kudinov, I. (2022). *The state of scientific development of innovative analytical and statistical technologies as a tool for corruption prevention*. Матеріали XII Міжнародної наукової конференції «Соціальне прогнозування та проектування майбутнього: зміни глобальної безпеки як виклик миротворенню та медіації» (10 червня 2022 року, м. Запоріжжя). Запоріжжя : ЦНСД, 99-101. URL: https://socforecast.org.ua/wp-content/uploads/socforecast2022.pdf

7. Яцина, Ю. (2019). *Проблемна ситуація наукового дослідження як основа для формулювання гіпотез*. Матеріали IX Міжнародної наукової конференції «Соціальне прогнозування та проектування майбутнього країни: проблеми мира та ненасильства в змінах глобального порядку» (12 квітня 2019 року, м. Запоріжжя). Запоріжжя : КСК-Альянс, 92-93. URL: https://socforecast.org.ua/wp-content/uploads/socforecast2019.pdf

8. Yatsyna, Y. (2017). *Cluster modeling as a tool for corruption counteraction in the state*. Матеріали VII Міжнародної наукової конференції «Соціальне прогнозування та проектування майбутнього країни: ідеї миру та ненасильства у змінах глобального порядку» (24 березня 2017 року, м. Запоріжжя). Запоріжжя : КСК-Альянс, 97-98. URL: https://socforecast.org.ua/wp-content/uploads/socforecast2017.pdf

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

АІС – автоматизована інформаційна система

АСК – автоматизована система контролю

АСУ – автоматизована система управління

ЗМІ – засоби масової інформації

ІКТ – інформаційно-комунікаційні технології

ІС – інформаційна система

ККУ – Кримінальний кодекс України

НАБУ – Національне антикорупційне бюро України

НАЗК – Національне агентство з питань запобігання корупції

САП – Спеціалізована антикорупційна прокуратура

ДАСУ – Державна аудиторська служба України

ООН – Організація Об’єднаних Націй

ОПР – особа, що приймає рішення

ПЗ – програмне забезпечення

СУБД – система управління базами даних

ШІ – штучний інтелект

ACFE – Асоціація сертифікованих фахівців з розслідування шахрайства (від англ. Association of Certified Fraud Examiners)

AI – штучний інтелект (від англ. artificial intelligence)

API – інтерфейс прикладного програмування (від англ. application programming interface)

CALS – система безперервного забезпечення життєвого циклу продукції (від англ. continuous acquisition and life-cycle support)

CPI – Індекс сприйняття корупції (corruption perception index)

CRM – система управління взаєминами з клієнтами (від англ. customer relationship management)

DLT – технологія розподіленого реєстру (від англ. distributed ledger technology)

DSS – система підтримки прийняття рішень (від англ. decision support system)

EIS – інформаційна система для керівництва (від англ. executive information system)

ERP – система планування ресурсів підприємства (від англ. enterprise resource planning)

FOSS – програмне забезпечення з відкритим вихідним кодом (від англ. free and open source software)

GenAI – генеративний штучний інтелект (від англ. generative artificial intelligence)

GII – Глобальний індекс доброчесності (global integrity index)

IT – інформаційні технології (від англ. information technology)

ML – машинне навчання (від англ. machine learning)

OLTP – обробка транзакцій в реальному часі (від англ. online transaction processing)

SCM – система управління ланцюгами постачання (від англ. supply chain management)

ВСТУП

Актуальність теми. В умовах повномасштабної війни, що триває в Україні з 2022 року, проблема корупції набула нової складності та гостроти. З одного боку, держава функціонує в екстремальних обставинах, коли необхідно оперативно ухвалювати рішення, мобілізовувати ресурси та підтримувати управлінську ефективність. З іншого – ризики зловживань у таких умовах зростають у рази, особливо у сфері розподілу гуманітарної допомоги, бюджетного фінансування, оборонних закупівель та публічного адміністрування. У цьому контексті зростає попит на інструменти, здатні забезпечити прозорість, підзвітність та раннє виявлення ризиків – тобто на інноваційні аналітико-статистичні технології.

Важливість розробки та впровадження таких технологій підтверджується і поточними даними щодо динаміки антикорупційної практики. Згідно з інформацією з Єдиного державного реєстру осіб, які вчинили корупційні правопорушення, лише 1,5% із 6 877 корупційних вироків, винесених з початку повномасштабної війни, завершилися реальними термінами ув'язнення. Переважна більшість осіб відбуваються штрафами, тоді як системні порушення – зокрема, у сфері декларування, конфлікту інтересів, незаконного збагачення – залишаються недослідженими або санкціонуються лише формально ("Since the beginning of the large-scale war, 6,800 corruption convictions have been handed down," 2024).

У 2024 році близько 35% вироків стосувалися порушень фінансового контролю, головним чином несвоєчасного подання декларацій, кількість яких зросла в 34 рази порівняно з попереднім роком ("Since the beginning of the large-scale war, 6,800 corruption convictions have been handed down," 2024). Це безпрецедентна динаміка, яка свідчить як про повернення до обов'язковості електронного декларування, так і про збої у системі контролю за доброчесністю посадовців. За визнанням НАЗК, значну частину справ було відкрито лише після

впровадження автоматичних перевірок і пріоритезації ризиків – тобто саме за допомогою інструментів аналітики та моделювання.

Додатковим підтвердженням актуальності теми є зміст і структура оновленого Реєстру корупціонерів. На кінець 2023 року він містив понад 44 тисячі записів, а основними підставами для внесення до реєстру є ті ж самі види правопорушень: фінансовий контроль, конфлікт інтересів і надання неправомірної вигоди. Проте в 86% випадків порушники отримали лише штрафи, і понад половина цих штрафів – мінімальні. Це свідчить про те, що реєстр відображає не боротьбу з корупцією, а її видиму адміністративну обробку, що не створює ефекту невідворотності покарання ("В Украине снова открыт Реестр коррупционеров," 2023).

Не менш симптоматичними є дані щодо іншого суміжного явища – зростання рівня шахрайства, що у низці випадків має корупційну природу (зловживання довірою, махінації з документами, підробка фінансових записів). У 2024 році в Україні було відкрито майже 65 тисяч кримінальних проваджень за статтею 190 ККУ («Шахрайство»), що в 2,7 рази більше, ніж у довоєнний період. Лише чверть цих справ було передано до суду ("Fraud cases decreased by 21% compared to the previous year," 2025). Така статистика вказує не лише на масштаб проблеми, а й на обмеженість ручних механізмів виявлення та реагування – що ще раз підкреслює необхідність впровадження автоматизованих аналітичних систем.

З огляду на масштабність проблеми, що фіксується і в кількісному, і в якісному вимірі, очевидним стає обмеження традиційних інструментів антикорупційної політики – як інституційних, так і юридичних. Фактична безкарність за більшість адміністративних правопорушень, формалізована практика наповнення реєстрів, фрагментарність реакції правоохоронної системи – все це вказує на потребу переходу до управління, орієнтованого на дані, з широким застосуванням цифрових інструментів аналізу, прогнозування, моделювання ризиків.

Аналітико-статистичні технології, зокрема засоби виявлення аномалій, DSS-системи підтримки рішень, моделі машинного навчання для прогнозування порушень – не лише створюють можливість підвищити ефективність державного контролю, а й змінюють логіку управлінських практик. Вони дозволяють формувати управлінські дії на підставі індикаторів і вірогідностей, а не лише ретроспективної реакції. Таким чином, мова йде не просто про технологічне вдосконалення, а про перехід до нового етапу антикорупційної політики – політики превентивного аналізу, ризик-менеджменту та цифрової доброчесності.

Усе це дає підстави стверджувати, що дослідження інноваційних аналітико-статистичних технологій попередження корупції в сучасній державі є надзвичайно актуальним. Воно відповідає не лише внутрішнім викликам України, а й глобальному тренду цифрової трансформації доброчесності, що передбачає переосмислення самої сутності боротьби з корупцією – не як покарання, а як управлінського проєктування прозорого середовища. У цьому контексті використання технологій набуває не технократичного, а стратегічного сенсу.

Проблемна ситуація, що стала основою для даного дослідження, полягає у тому, що попри активну цифровізацію державного управління в Україні, інноваційні аналітико-статистичні технології, які декларуються як інструменти попередження та протидії корупції, часто залишаються малоефективними або формальними. Цифрові реєстри, системи моніторингу, алгоритми виявлення аномалій та автоматизовані модулі оцінки ризиків не завжди інтегровані у реальні управлінські рішення. Більшість вироків за корупційні правопорушення мають м’який характер, значна частина систем залишається неузгодженою, а інституції – технологічно слабо оснащеними для глибокої аналітики. Це створює протиріччя між очікуваною ефективністю технологій і реальним рівнем їх впливу на зменшення корупції в публічному секторі.

Ситуація ускладнюється в умовах повномасштабної війни, яка з одного боку, вимагає пришвидшеного та ефективного управління ресурсами, а з

іншого – створює нові корупційні ризики, зокрема в галузі безпекових і соціальних витрат, гуманітарної допомоги, закупівель і відбудови. Водночас дані відкритих джерел (Єдиний державний реєстр корупціонерів, Opendatabot, звіти НАЗК) свідчать про істотне зростання кількості технічно зафіксованих, але не санкціонованих випадків правопорушень. Це свідчить про системну розбіжність між фіксацією та відповідальністю, між збором даних і їхньою реактивною інтерпретацією. Відповідно, доцільним є проведення комплексного аналізу технологій як потенційно ефективних антикорупційних інструментів, із урахуванням бар'єрів нормативного, інституційного та поведінкового характеру.

Ступінь наукової дослідженості проблеми свідчить про зростаючу актуальність тематики корупції, а також про активний розвиток інструментального та прикладного напряму в межах соціогуманітарного знання. Корупція як соціальне, політичне й економічне явище досліджується у низці наукових робіт, що розкривають її природу, причини, форми, інституційні умови виникнення, стратегії попередження та протидії. З-поміж українських дослідників варто виокремити О. Арабаджиєва, І. Басанцова, О. Зубарєву, С. Задорожного, І. Калугіну, М. Кікалішвілі, Д. Костенко, О. Костенко, Г. Кохан, І. Кушнарьова, О. Лозинського, М. Мельника, О. Новікова, В. Трепака, А. Приходько, Л. Удовику, які охопили як правові, так і політико-соціальні аспекти антикорупційної політики. Із зарубіжних робіт вирізняються праці Б. Гедінггеймера, М. Беблави, М. Джонстона, С. Роуз-Акерман, Е. Сичакової-Беблави, К. Стіфа, Ф. Фукуями.

Окремо слід окреслити роботи, присвячені тотожним тематиками, а саме корпоративному і фінансовому шахрайству. Серед вітчизняних авторів це роботи Д. Долбнєвої, Н. Ковтун, Ю. Хамиги, В. Чернєй; серед закордонних – Л. Вона, П. Годчолка, Дж. Гольдсроу-Вайт, Дж. Уелса.

Питання природи, функцій, проблем функціонування та трансформацій сучасної держави активно досліджуються вітчизняними та зарубіжними авторами у філософсько-правовому, політологічному та інституціональному вимірах. Серед вітчизняних дослідників варто відзначити Т. Бутченко,

В. Глазунова, Н. Горло, О. Кіндратець, В. Копча, О. Краснокутського, М. Лепського, Н. Лепську, М. Скибу, Н. Рикову, І. Терлюка. У зарубіжному науковому дискурсі це питання детально розглядається у працях Б. Джессопа, В. Джонатана, Д. Ігнатова, Н. Кірбі, Б. Родштейна.

Цифрова трансформація держави як окремий напрям досліджень набула особливого значення в роботах Г. Блінової, Н. Бабарикіної, В. Кривошеїна, Ю. Мальованої, А. Руднєвої, Л. Хорішко, Є. Цокура, І. Чайки. Серед закордонних дослідників в цьому напрямі виокремлюються роботи Дж. Брайтвайта, Я. Варуфакіса, П. Драхоса.

Наступний рівень досліджень – це ті, що стосуються загальних характеристик аналітико-статистичних технологій у контексті державного управління та суспільної трансформації. Зокрема, це роботи, які розглядають штучний інтелект, системи OLTP, алгоритми машинного навчання як інструменти для аналізу великих масивів даних. В даному напрямку переважають закордонні дослідники: Ч. Аггарвал, Б. Баесенс, Р. Берк, М. Гольдштейн, Л. Ертоз, І. Кудінов, Б. Ланз, С. Хан, Л. Чан, Й. Чен та ін.

Четверта категорія досліджень об’єднує роботи, що безпосередньо зосереджені на застосуванні аналітико-статистичних технологій для виявлення, запобігання або моніторингу корупційної діяльності. Прикладами є дослідження, присвячені аналізу структурованих баз даних державних закупівель (Й. Берру, В. Батиста, В. Вербека), розробці карт корупції на основі текстів новин (Д. Ноерліна, Ретно, Т. Мурсітама та ін.), створенню індексів корупційного висвітлення в медіа (С. Хлатшвайо, А. Оєкін, М. Жазанчан та ін.). Ці публікації поєднують NLP, графовий аналіз, візуалізацію даних та геоінформаційні системи.

Особливої уваги заслуговують експериментальні розробки, що апробують використання інформаційних технологій у реальних системах виявлення зловживань. Це, зокрема, система XPIV для виявлення шахрайства у сфері охорони здоров’я (Дж. Ліу, Е. Бір, А. Вілсон та ін.), аналітика на графах у сфері закупівель в Бразилії (Ц. Ралха, К. Сільва), а також роботи, які використовують

математичне моделювання для виявлення електоральних фальсифікацій (Дж. Клавер, П. Клімек, Д. Кобак, В. Мебане, А. Подлазов, М. Пшенічніков, С. Шпількін, Дж. Уол). Усі ці системи демонструють високу ефективність алгоритмів і свідчать про потенціал їх використання у державному секторі.

Дослідженнями в сфері впровадження інноваційних аналітико-статистичних технологій попередження злочинності, в тому числі, корупції активно займається низка дослідницьких інституцій, серед яких Центр незалежних соціологічних досліджень, Центр стратегічного прогнозування і проєктування, Український центр соціального планування, Союз соціальних технологів України та ін.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконана у межах науково-дослідної роботи кафедри політології Запорізького національного університету «Стратегічні технології державотворення: внутрішньополітичний та зовнішньополітичний виміри» (№ д/р 0121U111078) та «Стратегічні комунікації як інструмент реалізації національних інтересів держави: український та закордонний досвід» (№ д/р 0121U107470).

Об'єкт дослідження – держава в умовах цифрової трансформації публічного управління.

Предмет дослідження – інноваційні аналітико-статистичні технології як інструмент попередження корупції в державі.

Мета дослідження – визначити напрями оптимізації впровадження інноваційних аналітико-статистичних технологій попередження корупції в державі.

Завдання дослідження:

– уточнити зміст основних понять дослідження «попередження корупції» та «інноваційна аналітико-статистична технологія»;

– дослідити стан наукової розробки проблеми інноваційних аналітико-статистичних технологій попередження корупції в державі;

– обґрунтувати методологію дослідження проблеми інноваційних аналітико-статистичних технологій попередження корупції в державі;

– дослідити сутність держави як простору виникнення, розвитку і попередження корупції;

– визначити зміст та типи аналітико-статистичних технологій;

– проаналізувати аналітико-статистичні підходи до виявлення корупційних загроз в інформаційних системах держави;

– визначити напрями та технологічні платформи застосування аналітико-статистичних систем як інструменту попередження корупції;

– дослідити особливості впровадження інноваційних аналітико-статистичних технологій як інструменту попередження корупції в державі;

– розробити практичні рекомендації щодо впровадження інноваційних аналітико-статистичних технологій попередження корупції в Україні.

Методологічна основа дослідження. Під час написання роботи було використано низку загальнонаукових принципів, таких як: наукова обґрунтованість, об’єктивність, всебічність, історизм і комплексність. Саме ці принципи забезпечили цілісність дослідницької логіки, взаємозв’язок між теоретичним і емпіричним рівнями аналізу, а також дозволили уникнути редукціонізму в інтерпретації складних соціотехнічних явищ. У поєднанні вони дали змогу зберегти рівновагу між описом політичного контексту, розглядом інституційної дії та технічними характеристиками аналітичних інструментів.

Методологічною основою дослідження, яка дала змогу здійснити цілісний аналіз проблеми, став системний підхід, що надав можливість розглядати явище корупції в його взаємозв’язку з якістю врядування, ефективністю управлінських рішень, політичною відповідальністю та технологічною культурою.

Вагоме значення для дослідження мав інституційний підхід. Його сутність полягає в розгляді аналітико-статистичних технологій як таких, що функціонують не ізольовано, а в межах системи інституцій – таких як НАБУ, НАЗК, САП, ДАСУ, органи виконавчої влади, державні платформи електронного урядування. Цей підхід дозволив осмислити технологію як форму впливу на логіку прийняття рішень, механізми підзвітності та інструмент інституційного контролю.

Емпіричним методом дослідження було обрано експеримент по впровадженню інноваційних аналітико-статистичних технологій у пошукову роботу фахівців з протидії корпоративному шахрайству і корупції в межах навчально-виробничих практик студентів факультету соціології та управління Запорізького національного університету.

Наукова новизна одержаних результатів полягає у комплексному аналізі інноваційних аналітико-статистичних технологій попередження корупції в державному управлінні з урахуванням сучасного інституційного, політичного та цифрового контексту.

Уперше:

– здійснено міждисциплінарний аналіз інноваційних аналітико-статистичних технологій як специфічного інструменту антикорупційної політики в умовах цифровізації державного управління;

– визначено поняття «інноваційна аналітико-статистична технологія»: в широкому розумінні як сукупність методів та інструментів, що базуються на використанні математичних та статистичних методів аналізу даних з метою виявлення корисних залежностей та закономірностей в даних, підвищення ефективності прийняття рішень та виявлення аномалій у різних сферах діяльності; у вузькому – як процес використання найсучасніших методів та технологій аналізу даних, таких як машинне навчання, глибинне навчання, нейронні мережі, обробка природної мови, аналіз графів тощо з метою виявлення складних залежностей та корисних закономірностей в даних;

– розроблено сценарну модель розвитку цифрової антикорупційної інфраструктури в Україні, яка включає три варіанти (песимістичний, реалістичний, оптимістичний), та обґрунтовано умови їх реалізації з урахуванням політичної волі, нормативного середовища та цифрової культури.

Уточнено:

– сутність поняття «інструмент попередження корупції» – як цілісну систему аналітичних і статистичних дій, процедур чи технологій, які дозволяють

унеможливити виникнення або поширення корупційних проявів шляхом ранньої діагностики, прогнозування та зміни умов, що сприяють девіантній поведінці;

– типологію аналітико-статистичних технологій за функціональними блоками (збір, обробка, візуалізація, прийняття рішення, прогнозування) із виявленням залежності ефективності їх застосування від рівня інституційної інтеграції та прозорості алгоритмів;

– класифікацію цифрових практик у сфері боротьби з корупцією за змістом автоматизації: методологічне моделювання, аналіз вторинних даних, автоматизований текстовий аналіз і застосування машинного навчання, кожен з яких окреслює свій етап впливу на ухвалення управлінських рішень на місцевому, регіональному та національному рівнях.

Набули подальшого розвитку:

– уявлення про державу як подвійний інституційний простір: як джерело корупційних ризиків, так і механізмів стримування, з особливим акцентом на потенціал алгоритмічного врядування;

– уявлення про подвійний напрям антикорупційної технологічної дії: з боку інституційного ядра (органи влади, контрольні структури, урядові ІС) та з боку громадянського суспільства (активісти, журналісти, громадські платформи), які разом формують мережеву модель цифрового моніторингу;

– рекомендації щодо національної стратегії цифрового антикорупційного управління, що передбачає поєднання відкритих даних, алгоритмічного контролю, цифрової грамотності службовців та участі громадян у тестуванні інструментів публічної підзвітності.

Теоретичне та практичне значення результатів дослідження полягає, по-перше, у формуванні авторської інтерпретації сутності інноваційних аналітико-статистичних технологій як складового елементу сучасної антикорупційної політики держави. По-друге, запропоноване дослідження дозволило розширити уявлення про корупцію не лише як про правопорушення, а як про політичне, інституційне й поведінкове явище, яке потребує міждисциплінарного підходу, що поєднує інструменти аналізу даних, цифрового

моделювання, системного управління й політичної відповідальності. По-третє, результати дослідження поглиблюють теоретичну базу політичної науки в частині цифрової трансформації держави та модернізації інституцій публічного контролю. По-четверте, результати дослідження можуть бути впроваджені у викладанні навчальних дисциплін «Політологія», «Інформаційні технології в політології», «Державне управління та місцеве самоврядування» та при розробці нових навчальних дисциплін і спецкурсів у Запорізькому національному університеті. По-п’яте, авторські методичні рекомендації можуть бути використані як органами місцевого самоврядування України, так і обласними та районними державними адміністраціями для вдосконалення регіонального розвитку. Нарешті, шосте, результати дослідження впроваджені у діяльність ГО «Союз соціальних технологів України» (довідка № 28/05-1 від 28.05.2025 р.) та ГО «Український центр соціального проектування» (довідка № 28/05 від 28.05.2025 р.).

Особистий внесок здобувача полягає у тому, що сформульовані у дисертації положення та висновки отримані внаслідок самостійного дослідження.

Публікації. За результатами дисертаційного дослідження опубліковано 20 наукових праць, із них 11 статей, один розділ монографії та 8 тез конференцій.

Апробація результатів дослідження. Основні ідеї дисертації були оприлюднені під час науково-практичних конференцій: VII Міжнародна наукова конференція «Соціальне прогнозування та проектування майбутнього країни: ідеї миру та ненасильства у змінах глобального порядку» (24 березня 2017 року, м. Запоріжжя); IX Міжнародна наукова конференція «Соціальне прогнозування та проектування майбутнього країни: проблеми мира та ненасильства в змінах глобального порядку» (12 квітня 2019 року, м. Запоріжжя); XII Міжнародна наукова конференція «Соціальне прогнозування та проектування майбутнього: зміни глобальної безпеки як виклик миротворенню та медіації» (м. Запоріжжя, 10.06.2022 р.), XIII Міжнародна наукова конференція «Соціальне прогнозування та проєктування майбутнього: перемога, мир та відновлення у післявоєнній

Україні» (м. Запоріжжя, 28.04.2023 р.), Міжнародна конференція “Social Innovations for Sustainable Regional Development” (м. Клайпеда (Литва), 27-28.04.2023 року), IX Міжнародна науково-практична конференція студентів, аспірантів і молодих учених «Технології відновлення країни в умовах глобальних ризиків та невизначеностей» (м. Запоріжжя, 29.11.2024 року), XIII наукова конференція з нагоди Всесвітнього Дня Філософії (UNESCO) «Філософія і культура в антропологічних вимірах сучасності» (м. Дніпро, 22–23.11.2024 року), VIII Міжнародна науково-практична конференція «Інформаційне суспільство і Природа: вектори взаємовпливу» (м. Кривий Ріг, 21-22.11.2024 року); Всеукраїнська науково-практична конференція «Соціальні теорії та практики в контексті сучасної культури» (м. Дніпро, 25 квітня 2025 р.); XV Міжнародна науково-практична конференція «Соціальне прогнозування та проєктування майбутнього країни: людська суб’єктність vs штучний інтелект у миротворенні та повоєнному відновленні України» (м. Запоріжжя, 25.04.2025 року).

Структура та обсяг дисертаційного дослідження зумовлені метою і поставленими завданнями. Робота складається зі вступу, трьох розділів, дев’яти підрозділів, висновків і списку використаної літератури. До списку використаної літератури увійшли 334 позиції. Загальний обсяг роботи – 292 сторінок машинописного тексту, з них 211 сторінок становить основний текст.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПРОБЛЕМИ ІННОВАЦІЙНИХ АНАЛІТИКО-СТАТИСТИЧНИХ ТЕХНОЛОГІЙ ПОПЕРЕДЖЕННЯ КОРУПЦІЇ В ДЕРЖАВІ

1.1. Уточнення змісту основних понять проблеми інноваційних аналітико-статистичних технологій попередження корупції в державі

Почнемо наш аналіз з абстрактних понять, точніше понять, що не мають стійких тлумачень і мають таку ж розпливчасту сутність як і зміст реальної політики – з феномену корупція.

1. Корупція.

Причин тому декілька.

По-перше, феномен корупції – це «багатопланове і багатовимірне явище в структурі суспільних відносин, яке можна досліджувати у різних аспектах – економічному, культурному, соціологічному і, звісно, політичному» (*International Handbook on the Economics of Corruption*, 2006). Саме тому існує безліч визначень поняття «корупція», які використовуються в залежності від тих чи інших методологічних підходів, цілей і завдань дослідження.

По-друге, корупція як явище постійно адаптується до змін політичних, економічних і соціальних умов, а також до заходів протидії та боротьби з нею. «Надати однозначне визначення поняття корупції складно, оскільки воно проявляється по-різному, охоплює всю соціальну сферу, економіку, політику, культуру, мораль, право, психологію, владу, систему управління тощо» (Невмережицький, 2008, с. 44).

Термін корупція є похідним від латинських слів «corri» (обов'язкова причетність кількох представників однієї із сторін до справи) та «rumpere» (порушувати, ламати, пошкоджувати, скасовувати), які в подальшому утворили самостійний термін «corrumpere» для позначення діяльність кола осіб з метою перешкоджання судовому процесу або належному управлінню справами суспільства (Кікалішвілі, 2021, с. 27).

Як зазначає В. Трепак, в науковій літературі існує дві характерні особливості визначень корупції: 1) визначення, що «надто довільні та мало піддаються науковій оцінці, мають науково-популярний характер»; та 2) визначення, що «обмежені переказом «своїми словами» внутрішньо-нормативного або міжнародно-правового визначення корупції» (Трепак, 2020, с. 43).

Згідно з М.І. Мельником, корупція – це не тільки соціальне, а й психологічне явище. Воно не існує за межами поведінки та діяльності конкретних людей, спосіб життя яких визначається відповідним способом мислення (Мельник, 2001).

На думку М. Карпенко та В. Пашковського, корупція – це соціально-політичне явище, зміст якого представлено сукупністю нелегітимних дій осіб із владними повноваженнями, метою яких є задоволення особистих потреб та інтересів, що у кінцевому випадку приводять до корупційних злочинів (Карпенко & Пашковський, 2013).

Отже, загальновизнано, що публічна влада є джерелом, живильним середовищем і водночас основною сферою поширення корупції в державі. Поняття «корупція» в межах політичної сфери означає «підкуп» й «продажність» службовців, та представляє одну із форм відчуження «слуг народу» від безпосередньо народу (Марич, 2013).

З цього приводу С. Задорожний акцентує увагу на тому, що сутність корупції розкривається лише в системі «людина – публічна влада» шляхом виокремлення та розкриття п’яти кластерів ознак корупції як 1) виду державно-управлінських відносин; 2) правової девіації; 3) соціально-політичного інституту; 4) набору стратегій групової поведінки та 5) культурно-психологічного феномену (Задорожний, 2016). Корупційні взаємозв’язки, що призводять до викривлення економічного, соціального, політичного та іншого устрою, насамперед виникають у процесі взаємодії приватного сектору, громадян та їх об’єднань з органами публічної влади, її установами та

посадовими особами – у контексті регулювання суспільних сфер та надання публічних послуг.

З нормативної точки зору, сутність корупції полягає в «такому змісті антисоціальної поведінки, при якому дії, що порушують встановлене нормативне регулювання тієї чи іншої сфери діяльності, здійснюються шляхом використання публічних можливостей для реалізації особистих чи корпоративних інтересів на шкоду суспільним» (Трепак, 2020, с. 41).

В Україні згідно закону України «Про запобігання корупції» даний феномен визначається як «використання уповноваженими особами, перелік яких зазначений у Законі, своїх повноважень або тих можливостей, які службове становище надає особі задля отримання неправомірного доходу або обіцянка отримання подібного доходу іншій особі за умови виконання певних дій, що носять характер зловживання» ("Про запобігання корупції: Закон України від 14.10.2014 № 1700-VII," 2025). Однак, як зазначають деякі дослідники, цей феномен вже давно перетворився на транснаціональне явище ("Конвенція Організації Об'єднаних Націй проти корупції від 31.10.2003 р.," 2003).

Так, згідно Рекомендацій Rec (2001) 10 Комітету Міністрів Ради Європи з Європейського кодексу політичної етики під корупцією можуть розмітися такі дії як «підкуп, підробка або знищення доказів, фаворитизм, непотизм. Всі ці форми корупції обов’язково передбачають зловживання повноваженнями та посадою службовця» ("Європейський кодекс поліцейської етики. Рекомендація (2001) 10 Комітету Міністрів Ради Європи від 19 вересня 2001," 2001).

З юридичної точки зору корупція у широкому значенні – це «здатна до самовідтворення система суспільних відносин, що суперечать нормам суспільної моралі, та які виникають у зв’язку з несправедливим отриманням та/або перерозподілом благ особою, наділеною службовими повноваженнями, в інтересах осіб, що включені в цю систему, шляхом використання можливостей, які випливають зі службових повноважень» (Трепак, 2020, с. 52). У вузькому значенні корупція розуміється як «умисно вчинене особою, наділеною службовими повноваженнями, діяння (дію або бездіяльність), спрямоване на

отримання матеріальних та/або нематеріальних благ шляхом використання службового становища в особистих цілях, що визначене чинним законодавством як протиправне» (Трепак, 2020, с. 52).

На системність корупції вказує і М. Кікалішвілі, для якої корупція – це «складне системне явище, яке здійснює вплив на всі прошарки суспільства та змінює психологічні властивості учасників суспільного процесу» (Кікалішвілі, 2021, с. 104).

На думку М. Фоміної та В. Кузьменко корупція є видом відносин обміну, які «об'єднують окремих людей, різні інститути в єдиний соціальний організм». Відносини здійснюються за умов порушення формальних та / або неформальних норм, а метою цієї взаємодії є отримання послуг, що надають неправомірні переваги покупцям (фізичним і юридичним особам), а продавцям (посадовим особам держави, корпорацій, організацій) неофіційні прибуток (Фоміна & Кузьмеко, 2013, с. 184).

В свою чергу, Р. Тучак зосереджує увагу на трьох аспектах поняття «корупція»:

«а) політичному, який виражається в проникненні осіб кримінальної орієнтації в структури політичної влади і використанні їх можливостей для задоволення своїх злочинних потреб;

б) соціально-економічному, що полягає у спотворенні (викривленні) корумпованим держапаратом рішень держави з соціально-економічних питань, а також численними випадками допуску кримінальних елементів до економічних важелів управління;

в) правовому, для якого характерне лобіювання інтересів у процесі законотворчої діяльності» (Тучак, 2006, с. 204).

З кримінологічної точки зору, корупція – це «комплексне, укорінене, масове, системне суспільно небезпечне явище, зумовлене політичними, економічними, соціально-психологічними та іншими чинниками, що полягає у протиправному використанні публічно-владних повноважень та можливостей для задоволення приватних інтересів, а також у спонуканні до такого

використання чи сприяння йому. По суті, корупція є своєрідним способом конвертації публічно-владних повноважень і можливостей у неправомірну вигоду» (Трепак, 2020, с. 53) або злочини та/або правопорушення, пов'язані з використанням службового становища в особистих чи групових цілях.

Згідно Д. Костенко корупція – це «зловживання владою і/або службовим становищем задля одержання певної вигоди, що передбачає здійснення протиправної діяльності» (Д. В. Костенко, 2020, с. 29). За його думкою, корупція в будь-якій державі характеризується фактом зловживання службовим становищем з метою неправомірного одержання певного зиску або одержання пільг внаслідок необґрунтованого користування офіційним статусом. При цьому не має значення, хто був ініціатором обміну – зацікавлена сторона чи посадова особа. На думку автора, феномен корупції необхідно розглядати у трьох аспектах – соціальному, політичному та психологічному. Соціальна складова корупції обумовлена тим, що вона породжує відповідні форми суспільних відносин. Політична складова корупції обумовлена щонайменше двома чинниками: по-перше, тим, що суб'єкти корупційних діянь наділені політичною владою; по-друге, найвищою метою (політичної) корупції є захоплення й утримання влади, що надає можливість конвертувати суспільне благо у приватний зиск. Нарешті, психологічна складова корупції полягає у девіантній сутності, аномальності поведінки суб'єктів корупційної діяльності по відношенню до суспільних інтересів, суспільного блага, що формується у вигляді відношення суспільства до цього феномену та відповідних соціально-психологічних процесів у свідомості суб'єктів корупції (Д. В. Костенко, 2020, с. 31-35).

На думку О. Терещук корупції це двовимірний феномен: «1) як протизаконні діяння осіб, які уповноважені на виконання функцій держави, спрямовані на особисте збагачення; 2) стійкий зв'язок представників владно-управлінських структур зі злочинним середовищем і сприяння йому у проведенні протиправної діяльності за рахунок використання наданих державою повноважень» (Терещук, 2000, с. 9).

За С. Рогульським, «корупція – це незаконне прийняття майнових та немайнових послуг, благ і переваг особами, що уповноважені на виконання державних функцій, або особами, що відповідно до закону прирівнюються до них, з використанням свого правового статусу та пов'язаних з ним можливостей, а також підкуп зазначених осіб шляхом незаконного надання їм фізичними та уповноваженими представниками юридичних осіб цих благ, послуг та переваг з метою отримання від осіб, уповноважених на виконання державних функцій, або осіб, що прирівнюються до них, певних привілеїв» (Рогульський, 2005, с. 17).

Свою класифікацію підходів до розуміння сутності та змісту корупції надає О. Лозинський: економічний, політичний, юридичний, історичний та психологічний:

«а) як незаконний механізм соціально-економічного обміну між представниками влади та бізнесу, що має для них певну вартість і економічну доцільність;

б) як зловживання (перевищення) владою, службовим становищем, як атрибут функціонування влади (її бюрократичних інституцій) за різних форм політичного урядування;

в) як адміністративне правопорушення, що тягне за собою штраф та тимчасове відсторонення від виконання діяльності;

г) як технологія швидкого, несправедливого, незаконного збагачення та зміцнення нечисленних соціальних груп – олігархії;

д) як прихована протиправна діяльність публічних (політичних, посадових) осіб, зумовлена специфічними особливостями психології особистості та масовою психологією» (Лозинський, 2021, с. 28-33).

Згідно з позицією Л. Удовики та І. Калугіної (Udovyka & Kaluhina, 2025), корупція – це багатогранне соціально-правове явище, що вкорінюється у всіх сферах суспільного життя й деформує їхню природу. Корупцію слід розглядати в кількох вимірах: як соціальне явища, яке впливає на структуру й динаміку суспільства; як кримінологічну категорію, що включає протиправні дії, пов'язані з використанням службових повноважень для особистої вигоди; і як правове

явище, що формалізується в національному та міжнародному законодавстві через описові або перелікові визначення.

Автори зазначають, що корупція є не лише діями окремих осіб, а й цілими системами поведінки, що укорінюються й легітимізуються через політичні, економічні й культурні практики. Вони підкреслюють двосторонній характер корупційних відносин: у центрі завжди стоїть своєрідна «угода» між тим, хто має владу чи ресурси, і тим, хто прагне їх отримати. Такий підхід дозволяє авторам говорити про корупцію як про системну проблему, що не зникає сама собою, бо є глибоко інтегрованою у владні відносини, економічні практики й навіть соціальні очікування.

Корупція з точки зору економіки у широкому розумінні визначається як соціально-економічний феномен, породжений тіньовими економічними відносинами між посадовими особами та зацікавленими сторонами з метою задоволення особистих інтересів через комерціалізацію суспільних благ і цінностей. У вузькому сенсі корупція визначається як процес комерціалізації посадовими особами своїх функціональних обов'язків (Мазур, 2005, с. 36).

Три підходи у розумінні корупції визначає І. Валюшко. Згідно першого підходу, корупція – це протиправне корисливе діяння, що вчиняється особою, яка наділена владними повноваженнями. Другий підхід акцентує увагу на корупції як невід'ємним супутником економічних відносин, який сприяє прискоренню роботи адміністративної машини. Третій підхід стверджує про асоціальну сутність корупції, як комплексі протиправних неетичних дій (Валюшко, 2013).

Одним із напрямків досліджень феномену корупції є дослідження механізмів попередження та протидії корупції в державі. До цього напряму відноситься, наприклад, дослідження С. Задорожного (Задорожний, 2016). Автор окреслює основні підходи до дослідження феномену корупції, серед яких вирізняються: традиційний, орієнтований на нормативно-ціннісне розуміння корупції; модерністський, що тяжіє до класичних уявлень про відхилення від публічного інтересу; неокласичний, який пропонує гнучкіші аналітичні рамки;

економічний або ринково-центристський, що трактує корупцію як результат раціонального вибору в умовах недосконалого регулювання; ревізіоністський або функціональний, який акцентує на потенційних адаптивних функціях корупції; політологічний, зосереджений на зв'язку між корупцією та структурою влади; біхевіористичний, що інтерпретує її як форму масової девіантної поведінки; а також інституційний, який аналізує механізми її відтворення в межах публічного управління.

Всі існуючі дефініції поняття «корупція» автором систематизовано у п'ятьох кластерах: «як особливого виду державно-управлінських відносин; як правової девіації; як соціально-політичного інституту, певного системного явища; як культурно-психологічного феномену; як відповідного набору стратегій поведінки різного роду соціальних груп, що прагнуть отримати незаконні переваги й преференції через використання влади та службового положення» (Задорожний, 2016, с. 70-72).

Найбільш поширеного використання отримало визначення корупції ("What is Corruption?,") як «зловживання публічною владою заради отримання приватної вигоди». Це дуже узагальнене визначення, завдяки якому в якості корупції можна вважати будь-які дії посадових осіб, метою яких є отримання власної вигоди. Тобто метою яких може бути як надання необґрунтованої переваги третім особам (наприклад, під час проведення тендерних закупівель), так і дії, пов'язані із задоволенням, наприклад, почуттів помсти підлеглого по відношенню до керівника. Останній приклад дій посадових осіб кваліфікується як шахрайство. Тому зрозумілим є ототожнення корупції із шахрайством, яке можна тлумачити як «1) хитрий і спритний обман; крутійство; ошуканство; 2) заволодіння індивідуальним майном громадян або набуття права на майно шляхом обману чи зловживання довірою» (*Великий тлумачний словник сучасної української мови*, 2007, с. 1615) або навмисну дію «одного або більше осіб серед керівництва, управлінського персоналу, співробітників або третіх сторін, що полягає у використанні обману для одержання неправомірної або незаконної вигоди» (*International Standard on Auditing 240: The Auditor's Responsibilities*

Relating to Fraud in an Audit of Financial Statements, 2010). Міжнародна аудиторська компанія «PricewaterhouseCoopers» трактує шахрайство як «навмисний обман з метою розкрадання грошових коштів, майна або законних прав» ("Всемирный обзор экономических преступлений," 2011). За методологію ACFE, шахрайство (а точніше корпоративне шахрайство) – це «використання службового становища з метою особистого збагачення шляхом навмисного неналежного використання або зловживання ресурсами і активами організації-роботодавця» (*Occupational Fraud 2022: A Report to the Nations*, 2022, с. 6).

Окремою категорією шахрайства є шахрайство з фінансовими ресурсами. Вітчизняний вчений В. Чернєй виділяє дві основні «групи злочинів у сфері державних фінансів: 1) посягання, безпосередньо спрямовані на державні фінанси (статті 190, 191, 199, 204, 210, 211, 212, 212–1, 216, 222, 233 ККУ); 2) пов'язані з ними злочини, що є складовими способу їх підготовки, учинення або приховування (статті 200, 205, 209, 209–1, 219, 222–1, 223–1, 223–2, 224, 358, 361, 361–2, 364–367 ККУ)» (Чернєй, 2014, с. 5). С. Чорнуцький оперує терміном «шахрайство по відношенню до державних ресурсів» та визначає його як «навмисно допущені порушення законодавства (порушення, допущені з метою отримання власної вигоди чи вигоди третіх осіб), що призвели до шкоди внаслідок втрати державних ресурсів чи їх недоотримання» (Чорнуцький, 2011, с. 129).

На думку Ю. Хамиги, під поняттям «шахрайство з фінансовими ресурсами держави» слід розуміти «сукупність економічних відносин між юридичними чи фізичними особами і державою в процесі формування, розподілу і використання її фінансових ресурсів, які реалізуються шляхом обману або зловживання довірою чи службовим становищем з метою отримання економічної або/та іншої вигоди (особистої, корпоративної чи на користь третіх осіб), і призводять до втрати (зменшення, недоотримання) державних ресурсів внаслідок незаконного їх використання» (Хамига, 2020, с. 107).

В цілому, в нашому дослідженні під корупцією ми будемо розуміти протиправне використання посадовою особою наданих їй управлінських

ресурсів для особистої чи групової вигоди, що може мати як матеріальну, так і нематеріальну форму. При цьому протиправне використання – це порушення як формальних нормативно-юридичних установ, включаючи норми службової поведінки та етики, так і неформалізованих норм поведінки, етики і моралі.

2. Попередження корупції.

Продовжуючи наш аналіз, ми переходимо до словосполучення «попередження корупції». Сучасні науковці також досі не визначилися з усталеним семантичним позначенням соціальної діяльності, спрямованої на обмеження корупційних практик. У науковій та прикладній літературі вживаються різні поняття: «протидія корупції», «запобігання корупції», «боротьба з корупцією», «профілактика корупції», «антикорупційний контроль» тощо. Таке термінологічне різноманіття є не лише наслідком багатозначності соціального феномену, а й свідченням гносеологічної незавершеності у витворенні адекватного понятійного апарату.

Вважаємо за доцільне окремо розглянути не лише семантику поняття «попередження корупції», а й виокремити теоретичне визначення словосполучення «інструмент попередження корупції». Йдеться не просто про дії чи заходи, що мають протидіючий або реактивний характер, а про інтегровані технологічні чи управлінські механізми, спрямовані на створення середовища, у якому потенційні ризики виникнення корупційної поведінки виявляються, нейтралізуються або відвертаються ще до того, як набудуть форми правопорушення. Таким чином, під інструментом попередження корупції ми розуміємо цілісну систему аналітичних і статистичних дій, процедур чи технологій, які дозволяють унеможливити виникнення або поширення корупційних проявів шляхом ранньої діагностики, прогнозування та зміни умов, що сприяють девіантній поведінці.

Водночас для повноти дослідження варто звернутися до наявного спектру інтерпретацій таких термінів як «протидія» та «запобігання», адже саме через їх гносеологічне порівняння проступає зміст категорії «попередження». Наприклад, згідно з Великим тлумачним словником сучасної української мови,

«протидіяти» означає спрямовувати діяльність проти чого-небудь, діяти всупереч чомусь. Відповідно, «протидія» – це сукупність дій, спрямованих на здійснення опору чи перешкод іншим діям, часто з моментом фактичної зустрічі з об’єктом небажаної діяльності (*Великий тлумачний словник сучасної української мови*, 2007, с. 1173). У цьому сенсі протидія є реактивною стратегією.

Зазвичай під поняттям «протидія корупції» розуміють «антикорупційну діяльність органів державної влади, органів місцевого самоврядування, інститутів громадянського суспільства, організацій і фізичних осіб в межах їх повноважень», а під механізмом запобігання й протидії корупції – «цілеспрямовані скоординовані антикорупційні дії зазначених суб'єктів державно-владних відносин, спрямовані на попередження, викриття та покарання корупційних дій в системі публічного управління» (Задорожний, 2016, с. 28).

На думку О. Новікова, протидія корупції – це «діяльність у сфері публічного управління з метою зменшення можливостей для корумпованості суспільних відносин» (Новіков, 2020, с. 53). При цьому у науковому просторі протидія корупції має вузьке та широке значення. В першому випадку це система заходів, спрямованих на зменшення обсягів корупції, обмеження впливу корупції на інші соціальні явища та процеси, а також дії щодо нейтралізації чинників корупційної поведінки, застосування санкцій до суб’єктів корупційних правопорушень та усунення їх наслідків. Широке розуміння протидії корупції тлумачиться як «правомірна діяльність, яка сприяє зменшенню можливостей для таких дій, зокрема шляхом забезпечення верховенства права, реалізації інших принципів права, розвитку демократичного суспільства та утвердження правової держави» (Новіков, 2020, с. 54).

На відміну від цього, «попередження» як категорія має конструктивний, випереджувальний характер. Його суть не у зменшенні наслідків уже проявленого явища, а в такому перетворенні умов соціальної взаємодії, яке виключає або мінімізує можливість виникнення девіантної поведінки. Слід зауважити, що «попередження» не є синонімом «запобігання», що радше має

контекст ситуативного уникнення, а є системною діяльністю з випереджального виявлення ризиків і формування середовища антикорупційної несприйнятливості.

Згідно із дослідженням А. Приходько, запобігання (або в нашому випадку попередження), протидія та боротьба це три різні напрями антикорупційної діяльності. Запобігання та боротьба з проявами корупції в державі передбачає сумісну активність всіх зацікавлених суб'єктів (держави, бізнесу, громадського суспільства) щодо «виявлення, вивчення, обмеження або усунення явищ, що породжують корупційні правопорушення або сприяють їхньому поширенню … всіма доступними способами комунікативної взаємодії, реалізація якої об'єктивована превентивними, репресивними та ліквідаційними заходами», то протидія – це суто діяльність «антикорупційних і правоохоронних органів, спрямована на виявлення корупційних правопорушень, належне розслідування, притягнення до відповідальності правопорушників, а також захист осіб, яким заподіяно шкоду внаслідок корупційних дій» (Приходько, 2020, с. 140-141).

Етимологічний і семантичний аналіз словникового визначення терміну «попередження» ("Попередження,") свідчить про багатозначність цього поняття, однак у межах нашого дослідження нас цікавить передусім третє значення – «запобігання вияву чого-небудь небажаного». Саме це значення найадекватніше відображає гносеологічну суть поняття «попередження корупції», оскільки дозволяє мислити попередження як діяльність, орієнтовану не на реакцію чи санкцію після факту порушення, а на усунення передумов його виникнення.

Як можна побачити з наведених у словнику прикладів, «попередження» вживається і як повідомлення (наприклад, про небезпеку), і як застереження, і навіть як наказ або погроза. Усі ці значення мають спільне ядро – часову випереджальність щодо очікуваної або прогнозованої події, що може становити загрозу, порушення або шкоду. Вже на цьому рівні «попередження» фіксує логіку причинно-наслідкового мислення, в якому суб'єкт діяльності, отримавши доступ до інформації про можливі наслідки, здійснює дію до моменту їх настання.

Особливо показовим є третє значення, у якому «попередження» трактується як соціальна практика, спрямована на запобігання аморальним або протиправним вчинкам. У цьому розумінні попередження має не тільки випереджальний, але й педагогічний, нормативний характер – воно включає у себе не лише дію, але й мету: трансформацію потенційно девіантної поведінки у напрямі соціально прийнятного результату. Такий підхід повністю відповідає концептуальній рамці нашого дослідження, де аналітико-статистичні технології постають не як каральні чи слідчі засоби, а як системи прогнозування, діагностики та управлінського втручання, які запобігають реалізації корупційного потенціалу.

Нарешті, вважаємо за необхідне взяти за аксіому твердження про те, що корупцію як феномен знищити неможливо, тому її неможливо побороти. Єдине, що можна з нею зробити, так це попереджати або протидіяти її розповсюдженню. Так, в одному з посібників «Антикорупційний комплаєнс» поняття протидії корупції розглядається, як діяльність суб'єктів антикорупційної діяльності щодо запобігання корупційним проявам (виявлення та намагання усунення причин поширення корупційної злочинності); боротьби з корупційними діяннями (їх припинення, розкриття та безпосереднє розслідування) та мінімізацію і ліквідацію наслідків вчинених корупційних правопорушень (Окунєв, Бойко, & Лукін, 2018).

Виходячи з цього, ми можемо сформулювати авторське визначення терміну «попередження корупції» як системи цілеспрямованих дій, методів, процедур або технологічних рішень, спрямованих на виявлення, нейтралізацію або трансформацію соціальних, управлінських, інституційних і психологічних факторів, які потенційно сприяють корупційній поведінці, ще до того, як така поведінка набуде форми фактичного правопорушення.

Це визначення дозволяє вивести поняття попередження корупції з тіні суто правового чи санкційного тлумачення і ввести його у сферу стратегічного управління ризиками. Воно інтегрує у собі як нормотворчі, так і інформаційно-аналітичні компоненти, що дозволяє обґрунтувати легітимність інноваційних

інструментів моніторингу, статистичного аналізу, машинного навчання й соціального прогнозування як інструментів попередження, а не лише виявлення або документування порушень.

В будь-якому випадку інструменти попередження корупції є невід'ємною складовою антикорупційної політики. В нашому випадку, антикорупційної політики держави, яку можна визначити як сукупність заходів, стратегій, норм і принципів, розроблених та впроваджених державними органами з метою запобігання, виявлення, розслідування та забезпечення відповідної відповідальності за корупційні правопорушення. Антикорупційна політика включає в себе ряд інструментів, таких як законодавчі акти, адміністративні реформи, системи контролю та нагляду, а також механізми сприяння прозорості та залучення громадськості. Основною метою антикорупційної політики є забезпечення чистоти, доброчесності та ефективності державної служби, а також підвищення довіри громадян до державних інститутів (Schöberlein, 2019).

Від абстрактних понять та феноменів ми переходимо у світ, де невизначеність завжди отримує своє визначення – у світ математики та науки про інформацію, а саме до уточнення поняття «інноваційна аналітико-статистична технологія».

3. Інноваційна аналітико-статистична технологія.

Термін «аналітико-статистична технологія» може мати різні тлумачення, залежно від контексту, в якому він використовується. Однак, у загальному розумінні, це технологія, яка ґрунтується на застосуванні методів аналітики даних та статистичного аналізу для вирішення різних завдань у різних галузях.

У словниках технологію трактують:

«1) як сукупність знань, відомостей про послідовність окремих виробничих операцій у процесі виробництва чого-небудь;

2) як сукупність способів обробки чи переробки матеріалів, виготовлення виробів, проведення різних виробничих операцій тощо;

3) як науку про переробку і обробку матеріалів, способи виготовлення продукції та сукупність прийомів, застосовуваних у різних видах діяльності;

4) як будь-який засіб перетворення вихідних матеріалів, в якості яких можуть виступати: люди, інформація або фізичні матеріали – для отримання бажаної продукції чи послуг» (Олещук, 2019, с. 31).

Так, в одному з підручників з дифузії інновацій, під технологією розуміється «проект інструментальної дії, яка зменшує невизначеність причинних зв'язків на шляху до досягнення бажаного результату. Технологія, як правило, складається з двох компонентів: 1) апаратної частини (hardware), себто пристрою, який втілює технологію як матеріальний чи фізичний об'єкт, та 2) інформаційної частини (software), себто інформаційної бази цього пристрою» (Роджерс, 2009, с. 32). Тобто ми бачимо, що технологію можна розглядати в якості інструмента, характер використання якого визначається заздалегідь визначеною метою.

На думку П. Олещука, технологія це цілісна динамічна система, «що включає апаратні засоби, операції і процедури діяльності, управління цією діяльністю, необхідну для цього інформацію і знання, енергетичні, сировинні, кадрові та інші ресурси, а також сукупність економічних, соціальних, екологічних та інших наслідків, що певним чином впливають і змінюють соціальне і природне «середовище перебування» даної системи; сукупність процесів цілеспрямованої усвідомленої зміни, які утворюють взаємозалежні цикли логічно обумовлених перетворень речовини, енергії та інформації» (Олещук, 2019, с. 32).

В нашій роботі під терміном «технологія» ми будемо розуміти задокументований механізм або метод застосування певних фізичних або матеріальних об'єктів, функціонування яких заздалегідь визначено набором інструкцій.

Доволі схожим із технологією є термін «механізм». С. Задорожний досліджує механізм запобігання та протидії корупції в органах місцевої влади, під яким розуміє «комплекс реалізації послідовних дій щодо забезпечення взаємного впливу місцевих органів публічної влади, силових структур, інститутів громадянського суспільства та громадян в антикорупційній сфері, що

вирізняється партнерським характером взаємодії, відкритістю й прозорістю їх відносин та взаємовідповідальністю» (Задорожний, 2016, с. 8). Як можна побачити, механізм визначено як комплекс послідовно реалізованих дій (алгоритм) в сфері антикорупційної діяльності. По відношенню до технологій механізм є більш загальним, оскільки він передбачає орієнтацію на суб'єктів антикорупційної політики, в той час як технологія сконцентрована на більш матеріальних та повторюваних діях потенційних учасників корупційної діяльності.

Ми довго вагалися, який термін слід тлумачити першим – аналітика чи статистика. Зупинились на останньому у зв'язку із тим, що під даним терміном розуміється певна наука, тобто більше розроблена та досліджена на відміну від аналітики, що на даний час отримала лише статус дисципліни.

Одним із перших відомих літературних вживань слова «статистика» зустрічаємо у трагедії Вільяма Шекспіра «Гамлет» (акт 5, сцена 2, стих 35), де Гамлет говорить: "I once did hold it, as our statists do, A baseness to write fair" (Shakespeare, 2017). Тут слово «statist» означає не просто придворного, а людину, що займається державними чи політичними справами, хто розуміється на управлінні та владі. Походячи від латинського status («стан», «положення»), у цьому контексті воно позначає тих, хто, займаючи високе становище, дивиться зверхньо на «дрібниці» – як-от красиве письмо, – бо вважає себе причетним до справ вищого порядку.

На сучасному етапі розвитку суспільства термін «статистика» використовують у двох значеннях. По-перше, в побуті її розуміють як набір кількісних даних про якесь явище або процес. По-друге, фахівці в галузі статистичних методів називають «статистикою» функцію від результатів спостережень, що використовується для оцінювання характеристик та параметрів розподілу та перевірки гіпотез (Ewens & Brumberg, 2023; Siegel, 2016).

Слід зауважити, що застосування статистичних методів у складних системах неможливе за відсутності використання законів мислення, а точніше

аналітичних методів – аналітики. Аналітика постає як міждисциплінарний напрям, у межах якого взаємодіють три ключові складові: методологічні засади інформаційно-аналітичної діяльності, організаційна інфраструктура цієї діяльності та комплекс технічних і методичних рішень, що забезпечують створення інструментів для її реалізації.

До центральних елементів аналітичного процесу належать кілька послідовних та взаємозалежних дій. Насамперед це визначення управлінських цілей і постановка відповідних задач для інформаційно-аналітичної підтримки. Наступним кроком є гнучке, адаптивне управління процесом збору інформації з урахуванням змін у зовнішньому середовищі та потреб ухвалення рішень. Важливу роль відіграє інтерпретація зібраних даних у світлі поставлених цілей, що дозволяє глибше зрозуміти природу досліджуваних явищ і процесів.

Особливої ваги набуває побудова концептуальної моделі досліджуваного об’єкта, предметного поля або середовища, в якому він функціонує, разом із перевіркою її адекватності та подальшою корекцією за потреби. На цьому тлі здійснюється підготовка та реалізація емпіричних або модельних експериментів, спрямованих на збирання додаткових свідчень і перевірку гіпотез.

Завершальним етапом виступає синтез знання – тобто аналітична інтерпретація, формулювання висновків і прогнозів, які мають практичну цінність для управлінської діяльності. Результати цієї інтелектуальної праці доводяться до кінцевого користувача – суб’єкта управління або відповідного органу прийняття рішень.

Таким чином, аналітика постає як основа раціональної когнітивної діяльності, орієнтованої на вирішення прикладних задач і формування уявлень про майбутній стан досліджуваних об’єктів. Вона виконує інтегративну функцію, поєднуючи реконструкцію подій минулого, пояснення актуальних процесів та побудову прогнозів розвитку у майбутньому.

В цілому під аналітикою ми будемо розуміти «сукупність принципів методологічного, організаційного та технологічного забезпечення індивідуальної та колективної мисленнєвої діяльності, що дозволяє ефективно

обробляти інформацію з метою вдосконалення якості наявних та набуття нових знань, а також підготовки інформаційної бази для прийняття оптимальних управлінських рішень» (Захарова & Філіпова, 2013, с. 26-27).

Аналітика виступає як комплексна дисципліна, що поєднує методологічні підходи різних наукових напрямів, націлених на видобуток, коректне подання та управління знаннями. Вона інтегрує результати, які отримують у найрізноманітніших наукових галузях: від математики до синоптики та метеорології. Також аналітика включає деякі робочі методи з психології та психоаналізу, соціології, політології, історії, джерелознавства, бібліотечної справи, лінгвістики, педагогіки, криміналістики, юриспруденції та багатьох інших. Практично повний комплекс наук, які будь-коли робили спроби наукового інваріантного опису особливостей поведінки індивіда чи групи у різних ситуаціях: при груповій та індивідуальній діяльності, при викладанні думок, при синтезі цілей та виборі методів їх досягнень та інших ситуаціях.

Таким чином, в загальному сенсі під аналітико-статистичною технологією слід розуміти задокументовану процедуру або алгоритм аналізу даних. З погляду організатора прикладного аналітико-статистичного дослідження, можна виділити такі етапи аналітико-статистичного аналізу (Siegel, 2016):

– планування аналітико-статистичного дослідження;
– організація збору статистичних даних згідно програми дослідження;
– збір даних;
– первинний (статистичний) опис даних (середнє арифметичне, медіана, мода тощо);
– перевірка статистичних гіпотез;
– поглиблене вивчення статистик другого порядку (багатовимірний статистичний аналіз, моделювання, класифікація тощо);
– перевірка стійкості отриманих оцінок та висновків;
– застосування отриманих результатів у прикладних цілях;
– звітування.

Отже, можемо констатувати, що аналітико-статистичний аналіз даних – це інформаційно-технологічний процес, під час реалізації якого набори спостережень за певними об'єктами або їх властивостями (дані про них) піддаються різним операціям (послідовно, паралельно або по більш складним схемам). Тому на сучасному етапі розвитку людства неабияку роль у застосуванні статистичних методів відіграють інформаційні технології як найвищий рівень реалізації математичних (в тому числі, статистичних) технологій. Широке використання комп'ютерної техніки у всіх сферах діяльності організацій створює передумови активного застосування комп'ютерних технологій під час використання аналітико-статистичних методів в управлінні якістю.

Повернемося до аналітико-статистичних технологій, точніше до тих технологій, що мають статус інноваційних. Фахівець у галузі якості Каеру Ісікава поділяє аналітико-статистичні методи, що використовуються в системах якості, на три групи: елементарні, проміжні та передові. До елементарних методів належать звані «сім простих інструментів якості»: контрольний листок, гістограма якості, причинно-наслідкова діаграма, діаграма Парето, стратифікація, діаграма розсіювання, контрольна карта. Проміжні методи – це методи приймального контролю, теорії розподілів, статистичні оцінки та критерії. До передових методів належать методи, що базуються на використанні комп'ютерних технологій: планування експерименту, багатовимірний аналіз, методи дослідження операцій (Ishikawa, 1987, p. 198-199).

Нас цікавлять саме передові методи, оскільки вони мають безпосереднє відношення до інновацій. У сучасній літературі нараховується багато визначень інновацій. Найпростіше визначення інновації як ідеї, практики чи об'єкту, що «їх індивід або інший суб'єкт впроваджування сприймає як нові» (Роджерс, 2009, с. 31).

Термін «інновація» має своє походження від латинського слова «novator», що означає «оновлювач» – особа, яка впроваджує та реалізує нові, прогресивні ідеї, принципи чи методи в певній сфері діяльності. В англійській мові близьким

за змістом є дієслово «to innovate», що означає «впроваджувати нововведення» або «здійснювати зміни». У діловому контексті термін «innovator» використовується для позначення компанії, яка створює нові продукти або застосовує передові технології у виробничих процесах (Drucker, 1984).

Згідно із Законом України «Про інноваційну діяльність» інновації визначаються як «новостворені (застосовані) і (або) удосконалені конкурентноздатні технології, продукція чи послуги, а також організаційно-технічні рішення виробничого, адміністративного, комерційного або іншого характеру, що істотно поліпшують структуру та якість виробництва і (або) соціальної сфери» ("Про інноваційну діяльність : Закон України від 04.07.2002 №40-IV," 2023).

Узагальнивши, можна сказати, що у сучасних дослідженнях поняття «інновація» трактується здебільшого у межах двох підходів – статичного та динамічного. У межах першого, інновація розглядається як завершений результат, тобто «інновація-продукт» – новий виріб, технологія чи метод, що вже впроваджений на ринку. Натомість динамічний підхід акцентує увагу на процесуальній природі інновації як безперервному русі – від наукового дослідження, проєктування і розробки до організації виробництва, комерціалізації та розповсюдження новацій, що приходять на зміну наявним практикам (Гутуров, 2019, с. 16).

Слід врахувати, що в сучасній (насамперед, англомовній) науково-технічній літературі по відношенню до інноваційних технологій також використовується термін «hi-tech». Термін «високі технології» використовується для позначення найбільш передових технологій, що спираються на останні досягнення науково-технічного прогресу. Є такі технології і серед технологій аналітико-статистичного аналізу даних – як у будь-якій науково-практичній галузі, що інтенсивно розвивається.

Під високими аналітико-статистичними технологіями маються на увазі сучасні методи аналізу даних, що базуються на досягненнях теорії ймовірностей, прикладної статистики та аналітичної математики. До таких технологій належать

непараметричний аналіз, робасні (стійкі) підходи, методи розмноження вибірок, статистика нечислових і інтервальних даних. Їм протистоять так звані низькі аналітико-статистичні технології, які не відповідають актуальному рівню наукового розвитку, є застарілими та малопридатними до вирішення складних практичних завдань. Між цими двома полюсами розміщуються класичні методи, які, попри свій поважний вік, зберігають релевантність у сучасному статистичному аналізі (Яцина & Кудінов, 2021).

Існує й інший підхід (Köbis, Starke, & Rahwan, 2021; Odilla, 2023; Ковтун, 2011) до класифікації аналітико-статистичних технологій, згідно з яким їх можна поділити на традиційні (класичні) та автоматизовані. Перші передбачають діяльність 1-2 експертів із незначним застосуванням комп'ютерних (інформаційних) технологій, під час яких відбувається аналіз взаємозв'язків, взаємообумовленості різних показників з метою ідентифікації відхилень від норми (сюди можна віднести метод стереотипів, скорегованих показників, пов'язаних зіставлень тощо).

В свою чергу автоматизовані технології передбачають, по перше, залучення до процесу обробки даних інтелектуальні системи, що навчені виконувати аналітико-статистичні операції з наборами даних та спроможні замінити людину в більшості виконуваних операцій. До таких технологій відносять технології пошуку даних (data mining), ідентифікації в них аномалій (anomaly detection) або нового знання (novelty detection, knowledge discovery). Використанням цих алгоритмів дозволяє автоматизувати роботу декількох фахівців та спростити процес підготовки звітів про виняткові (нові, аномальні) ситуації. Виходячи з даної класифікації інноваційними аналітико-статистичними технологіями слід вважати автоматизовану групу технологій. Додамо, що використанням вказаних технологій в сучасних умовах розвитку суспільства неможливе без використання також таких технологій як машинне навчання (machine learning), глибинне навчання (deep learning), нейронні мережі (neural networks), обробка природної мови (natural language processing – NLP), аналіз графів (network analysis), аналізу даних у режимі реального часу (real-time data

analysis), які дозволяють отримувати швидкі та точні результати аналізу великих обсягів даних.

Наприклад, машинне навчання – це технологія аналізу даних, що дозволяє комп'ютерам вчитися, а також діяти як людина. Алгоритми машинного навчання використовують як аналітичні методи для «навчання» або отримання нового знання шляхом отримання даних, так і статистичні інструменти для пошуку закономірностей у великих обсягах даних. Під закономірностями розуміються в першу чергу зв'язки між певними характеристиками чи ознаками об'єктів, що досліджуються або дані щодо яких завантажуються та аналізуються. В цілому, метою машинного навчання є створення алгоритмів, що за допомогою статистичного аналізу спроможні самостійно обробляти значні за обсягами набори даних та передбачати на їх основі певні події.

Як зазначають (Köbis et al., 2021), активне впровадження технологій штучного інтелекту та машинного навчання дає нову надію на ефективнішу боротьбу з корупцією. Штучний інтелект суттєво відрізняється від статичних інформаційно-комунікаційних технологій. «Класичні» технології дозволяють цифровізувати процедури закупівель, надавати державні послуги онлайн та публікувати відкриті державні дані. Однак класичні технології не можуть діяти автономно, а штучний інтелект, навпаки, саме створений для цього. Завдяки своїм здібностям до навчання штучний інтелект може автономно виконувати широкий спектр завдань, раніше зарезервованих для людини (Rahwan et al., 2019). Саме в сучасних умовах цифрової трансформації держав штучний інтелект може взяти на себе антикорупційні завдання, такі як прогнозування, виявлення та розкриття корупційних справ (Lima & Delen, 2020; López-Iturriaga & Sanz, 2017).

Таким чином, при практичному використанні методів прикладної статистики та аналітики застосовуються не окремі методи опису даних, оцінювання, перевірки гіпотез, а розгорнуті цілісні процедури – так звані «аналітико-статистичні технології». Поняття «аналітико-статистична технологія» в нашому розумінні аналогічне поняттю «технологічний процес» у

теорії та практиці організації виробництва ("Методи вдосконалення технологічного процесу," 2022). Цілком природно, що одні статистичні технології краще відповідають потребам дослідника (користувача, статистика), інші – гірше, одні – сучасні, інші – застарілі, властивості одних вивчені, інших – ні. Аналітико-статистичний аналіз даних являє собою інформаційно-технологічний процес, у межах якого статистичні дані проходять різні етапи обробки – послідовно, паралельно або за складними комбінованими схемами – у рамках певної інформаційної технології.

Таким чином, за результатами уточнення змісту основних понять було отримані такі результати.

По-перше, уточнено зміст поняття «корупція» як багатовимірного феномену, що включає економічні, політичні, соціально-культурні, психологічні та правові аспекти. Жодне одне визначення не є достатнім для опису цього складного явища, адже воно постійно адаптується, змінюється під впливом контексту, політичних режимів, культурних кодів та соціальних практик. Саме тому ми систематизували підходи, позначивши його як правову девіацію, соціально-політичний інститут, культурно-психологічний феномен та набір стратегій групової поведінки.

По-друге, уточнено зміст словосполучення «попередження корупції». В межах дослідження ми свідомо розмежували його від близьких термінів, таких як «боротьба», «протидія» чи «запобігання» корупції. Запобігання корупції визначено як система цілеспрямованих дій, методів, процедур або технологічних рішень, спрямованих на виявлення, нейтралізацію або трансформацію соціальних, управлінських, інституційних і психологічних факторів, які потенційно сприяють корупційній поведінці, ще до того, як така поведінка набуде форми фактичного правопорушення. Попередження в нашому тлумаченні означає не обов’язкову фінальну перемогу чи знищення феномену, а постійний супротив, тривалу діяльність, що без часових обмежень спрямована на ускладнення, блокування й реагування на прояви корупції.

По-третє, особливу увагу ми приділили формулюванню терміну «аналітико-статистична технологія», розуміючи під ним задокументовану процедуру або алгоритм аналізу даних, що поєднує методи збору, обробки, аналізу, перевірки гіпотез, прогнозування й моделювання. Це не просто набір статистичних операцій, це цілісний інформаційно-технологічний процес, що забезпечує управлінські рішення на основі даних. На сучасному етапі цей термін охоплює як класичні (наприклад, методи аналізу вибірок, побудови статистичних моделей), так і передові інноваційні підходи – машинне навчання, глибинне навчання, обробку природної мови, аналіз графових структур тощо.

По-четверте, визначено поняття «інноваційні аналітико-статистичні технології» як поєднання передових методів аналізу даних, які дозволяють виявляти приховані закономірності, прогнозувати ризики й вчасно реагувати на потенційні або вже наявні загрози. Такі технології стають не просто засобом опису ситуації, а перетворюються на активний антикорупційний ресурс, що дозволяє інтегрувати аналіз даних у прийняття управлінських рішень на рівні держави. Ця концептуалізація є основою для подальших теоретичних і прикладних частин роботи, бо дає чіткі рамки для опису, аналізу й оцінки ефективності тих інструментів, які ми розглядатимемо в наступних розділах.

Нарешті, п’яте, визначено, що попередження постає як стратегічна, випереджальна діяльність, спрямована на усунення або модифікацію факторів ризику до моменту їхньої актуалізації у формі корупційної поведінки. В свою чергу, протидія – це вже безпосереднє інституційне реагування на виявлені або прогнозовані корупційні дії з метою їхнього обмеження, нейтралізації або санкціонування. У практичній площині ці дві категорії не є жорстко розмежованими: більшість ефективних управлінських і технологічних інструментів мають змішаний характер дії – вони одночасно виконують функції раннього виявлення загроз (превенція) і оперативного реагування на вже наявні корупційні прояви. Наприклад, системи предиктивного аналізу, виявлення аномалій у публічних даних, кластеризації корупційних ризиків або штучного інтелекту для моніторингу поведінкових шаблонів можуть застосовуватись як

для прогнозування й запобігання потенційним порушенням, так і для документування фактів, які вже вказують на здійснення корупційної практики. Тому з науково-прикладної точки зору (особливо в контексті нашої роботи) цілком виправданим є вживання узагальненого виразу «попередження / протидія корупції», який коректно репрезентує двоїстий – превентивно-реактивний – характер інноваційних технологічних рішень у сфері боротьби з корупцією.

1.2. Стан наукової розробки проблеми інноваційних аналітико-статистичних технологій попередження корупції в державі

Вважаємо за доцільне заздалегідь обмежити глибину аналізу першоджерел у зв'язку із тим, що тема дослідження безпосередньо пов'язана із інформаційними технологіями, які відрізняються достатньо швидкими темпами розвитку. Те, що вважалося інноваційною технологією десять років тому, вже є звичною справою сьогодні. Саме тому, глибина аналізу останніх досліджень за предметом нашого дослідження не буде перевищувати 10 років. Крім цього, аналізувати будемо не поодинокі праці (статті), а ґрунтовні дослідження – дисертаційні дослідження (дисертації, автореферати), монографії чи подібні до них публікації.

За предметом дослідження всі публікації можна умовно поділити на три групи, що сформовано за принципом переходу від абстрактного до конкретного, а саме:

1) корупції як загального суспільного явища;
2) корупції як протиправного діяння на робочому місці (шахрайство);
3) корупції як аномалії.

1. Корупція як загальне суспільне явище.

Перший тип робіт присвячено дослідженню загальних властивостей феномену корупції та напрямів боротьби з нею. Однією з перших робіт, в якій висвітлено тему застосування інноваційних технологій попередження / протидії корупції в державі, є дослідження (Басанцов & Зубарева, 2016). Автори монографії станом на 2016 рік висвітлили як світовий досвід антикорупційної

діяльності, а саме Японії, Південної Кореї, Сінгапуру, США, Грузії, так і України. Окремий розділ присвячено практикам протидії легалізації злочинних доходів («відмивання» грошей) в Україні та світі. Дослідження заслуговує на увагу у зв'язку з тим, що, у порівнянні з іншим, більш пізнішими вітчизняними дослідженнями, автори присвятили частину (розділ) саме інноваційним з їх точки зору технологіям попередження / протидії корупції, а саме питанням відкритості та прозорості діяльності органів державної влади, нормативно-правовому забезпеченню електронного врядування в Україні, аналізу сутності електронної взаємодії громадян і держави в системі «Е-уряд» та основам електронної демократії. Додатково автори торкаються таких тем як технології моніторингу та досліджень корупції інститутами громадянського суспільства, ролі ЗМІ, Інтернет та блогосфери та, нарешті, питання громадської експертизи як механізму попередження корупції. Читаючи наробки авторів у 2016 році та порівнюючи із досягненнями 2025 року, стає зрозуміло, як швидко розвиваються сучасні інформаційні технології і як вони впливають на можливості застосування аналітико-статистичних технологій.

Наступне дослідження (Задорожний, 2016) присвячене виявленню нових тенденцій і закономірностей корупційних відносин в системі органів публічної влади та розробка підходів до удосконалення механізмів попередження / протидії корупції в Україні на регіональному рівні. Робота викликає інтерес, в першу чергу, з теоретичної точки зору. Автором розкрито сутність та зміст корупційних відносин в системі «людина – публічна влада», шляхом виокремлення й розкриття п'яти основних кластерів ідентифікуючих ознаки корупції – як виду державно-управлінських відносин; як правової девіації; як соціально-політичного інституту; як набору стратегій групової поведінки та як культурно-психологічного феномену.

Автором виділяється 7 підходів до розуміння сутності та змісту феномену корупції:

1. Традиційний (нормативно-ціннісний) підхід, згідно з яким корупція є патологією політики, «соціальним злом, породженим глибинними соціальними

протиріччями суспільства, держави та її інститутів» (Куц, Сінченко, Мамонова, & Газарян, 2011, с. 303).

2. Модерністський (класичний), за яким корупція розуміється як протиправна дія (продажність) посадової особи органу публічної влади або «зловживання ввіреною владою для приватної вигоди» ("What is Corruption?," 2023).

3. Економічний (ринково-центристський), в якому корупція – це різновид економічної поведінки, метою якої є «максимізація корисності за допомогою вилучення непродуктивного доходу внаслідок маніпуляції ресурсами, що знаходяться в розпорядженні посадових осіб органів публічної влади відповідно до їх посадових повноважень» (Rose-Ackerman & Palifka, 2016, p. 14). Представники даного підходу вважають крайньою формою прояву корупції так званий ефект «state capture» (захоплення держави) – об'єднання економічної та політичної корупції, спроможної вразити найвищі рівні публічної влади, що призводить до стрімкої делегітимізації всієї системи публічної влади.

4. Ревізіоністський (функціональний) підхід, згідно з яким корупція є невід'ємною складовою суспільств, що розвиваються. Корупція – це хвороба невідповідності між старими правовими нормами та новими моделями поведінки, що встановлюються в транзитивній країні, сприяє «соціальній та політичній інтеграції в суспільствах, задовольняючи потреби, які залишилися поза офіційними процедурами» (A. Heidenheimer, Johnston, & Levine, 1989, с. 362-363). Корупція в державах із сильними авторитарними тенденціями навіть може стабілізувати політичну системи за рахунок посилення опозиції, яка в інших умовах може бути позбавлена доступу до держави (Huntington, 1968).

5. Політологічний підхід, що концентрує увагу на корупції як формі використання влади посадовими особами (держслужбовцями), промислово-фінансовими групами, суспільно-політичними рухами, партіями тощо для впливу на політичні процеси в країні. Підхід передбачає, що основною причиною корупції є нестача демократії в суспільстві, а її наслідком – деформація демократичних інститутів та тяжіння до авторитаризму. На думку О. Стогової

корупція є «неформальним інституційним середовищем економічних, адміністративних і інформаційних ресурсів, у якому владні еліти взаємодіють між собою та іншими структурами суспільства. Характер тіньового обміну ресурсами між владою і бізнесом та результат боротьби між ними фактично визначають тип політичного режиму у нових незалежних країнах, що трансформуються. У політичних системах, які трансформуються, створення корупційної мережі дозволяє встановити неконкурентний політичний режим, що сприяє корупції на всіх рівнях політичного процесу» (Стогова, 2016, с. 169).

6. Біхевіористичний (соцієтально-психологічний) підхід фокусує увагу на аналізі чинників корупційної поведінки для різного роду суб'єктів. Корупція за такого підходу «є поєднанням таких пороків людини як жадібність, заздрість, лінь, невгамовна спрага насолод тощо» (Невмережицький, 2008, с. 143). З точки зору даного підходу найбільша загроза корупції є те, що «вона є потужним фактором деморалізації суспільства, девальвації моральних цінностей, нищить духовні та моральні устої, тобто стає основним чинником загрози національній безпеці» (Нинюк & Нинюк, 2015, с. 73).

7. Інституційний (державно-управлінський) підхід, що визначає корупцію як «особливу форму державно-владних відносин, змістом яких є нелегальні обміни службовими повноваженнями посадових осіб органів публічної влади, які націлені на задоволення їх особистих або груп, які вони представляють, що тягне за собою розширення можливостей ведення бізнесу з боку задіяних учасників корупційних відносин та незаконного обмеження для тих, хто не є їх учасником» (A. J. Heidenheimer & Johnston, 2011, с. 15). А отже, «корупція виступає покажчиком ентропії державно-управлінської системи, певним виміром управлінської неефективності органів публічної влади в окремих галузях, сферах, безпосередньо в місцях надання адміністративних послуг – скрізь, де індивід вступає у відповідні відносини з представниками місцевої влади» (Задорожний, 2016, с. 26).

8. Синергетичний підхід, як органічне поєднання усіх попередніх, що тлумачить корупцію як стан 1) деформації державного управління;

2) олігархізації; 3) делегітимізації органів публічної влади; 4) порушення законних прав громадян на користь окремих осіб або груп осіб всупереч суспільним і державним інтересам; 5) фактичної залежності громадян від свавілля недоброчесних держслужбовців; 6) зневіри громадян, поширення нігілізму, деструктивних моделей поведінки тощо (Задорожний, 2016, с. 27-28).

Також автором систематизовано підходи до розуміння феномену корупції за п’ятьма ідентифікуючими ознаками (кластерами). Перший зосереджується на ній як на специфічному різновиді державно-управлінських відносин, акцентуючи увагу на взаємодії органів публічної влади та посадових осіб із громадянами в процесі надання адміністративних послуг. Другий підхід трактує корупцію як порушення норм службової етики, правових процедур і моральних приписів. Третій розглядає її як соціально-політичний інститут, що функціонує паралельно до легітимної державно-правової системи, охоплюючи широкий спектр форм зловживання владою. Четвертий кластер інтерпретує корупцію як культурно-психологічний феномен, що коріниться в природі людини й реалізується залежно від рівня її культурного й громадянського розвитку або в межах, або поза межами соціально-нормативних обмежень. Нарешті, п’ятий підхід розглядає корупцію як набір поведінкових стратегій впливових груп – фінансово-промислових кланів, політичної еліти, лобістських організацій – які прагнуть отримати нелегітимні переваги через маніпуляцію владними повноваженнями (Задорожний, 2016, с. 72).

Однак, не зважаючи на достатньо теоретичну обґрунтованість, в дослідженні С. Задорожнього залишилася поза увагою тема використання інноваційних технологій взагалі та аналітико-статистичних технологій зокрема. Наявні лише натяки на це (Задорожний, 2016, с. 132).

Під час аналізу становлення системи попередження / протидії корупції в Україні автором виокремлено й охарактеризовано один з етапів, що характеризується запровадженням системи електронного декларування. Серед напрямків оптимізації зазначено необхідність створення систем анонімного зворотного зв’язку з громадянами (Задорожний, 2016, с. 162) та «безконтактні»

адміністративні послуги, при яких виключено прямий контакт між громадянином і представником влади (Задорожний, 2016, с. 190).

Наступне дослідження має безпосереднє відношення до політичної корупції (Кушнарьов, 2018). У дослідженні проаналізовано типові форми політичної корупції, зокрема неправомірне забезпечення фінансування партійної діяльності; спроби викривлення інституційної ролі політичних партій у демократичному устрої; порушення етичних стандартів депутатами та високопосадовцями; торгівля місцями у виборчих списках з високими шансами проходження; організація підкупу виборців; використання владних повноважень у передвиборчій боротьбі; ухвалення партійних рішень без належної внутрішньої комунікації; ігнорування стандартів уникнення конфлікту інтересів серед осіб, що обіймають владні чи представницькі посади; застосування патронажних схем; прояви політичного непотизму, кронізму і фаворитизму; лобіювання, що не супроводжується публічністю або належним регулюванням; а також тиск або вплив на судову владу з політичних мотивів.

Найбільш цінними для нашого дослідження виявилися ті підрозділи, в яких автор розглядає сучасний стан розвитку систем попередження / протидії корупції у світі. Це стосується, по-перше, аналізу корупції в Естонії – досвіду мінімізації корупції завдяки побудові інноваційної моделі е-держави. За словами автора, «така модель максимально мінімізувала особистісний чинник у взаєминах громадянина, організації, компанії з чиновником» (Кушнарьов, 2018, с. 217). «А чи не найважливішим чинником успіху в досягненні низького рівня корупції в Естонії є прозорий процес прийняття рішень» (Кушнарьов, 2017, с. 97).

По-друге, досвід антикорупційної діяльності, а саме краудфандинговий проект «РосПил» (http://rospil.info/), сайту «Чорний блокнот» (http://blackbook.wiki/), сайту аналізу муніципальних кланів (https://petrograd.fbk.info/), проект «Декларатор» (http://declarator.org/).

По-третє, реформаторський досвід Грузії, щодо якого автором висловлені деякі сумніви: «корупцію було мінімізовано насамперед на рівні надання державних послуг, у сфері оподаткування, але це не може бути підставою

проекції такого результату на площину політичної корупції» (Кушнарьов, 2018, с. 296).

Наступна робота, що викликала значній інтерес, це дисертаційне дослідження В. Трепак щодо теоретико-прикладних проблем запобігання та протидії корупції в Україні. На думку автора, для кожної держави можна визначити так званий «суспільно допустимий рівень корупції», що виступає реалістичною метою (очікуваним результатом) протидії їй» (Трепак, 2020, с. 11). Найбільш цінне для нашого дослідження виявився огляд концепції «корупційна схема», яку зазвичай має ідентифікувати та чи інша аналітико-статистична процедура.

Автором достатньо якісно розроблено механізм протидії корупції в Україні, а саме визначені цілі, суб'єкти та об'єкти протидії корупції та форми і способи протидії корупції. Так формами протидії корупції є запобігання та боротьба з корупцією, з чого випливає, що інноваційні аналітико-статистичні технології можуть застосовуватися лише у формі боротьби з корупцією, а саме при виявленні (розкритті) фактів вчинення корупційних діянь та встановленні підозрюваних у їхньому вчиненні.

Що стосується аналітико-статистичних технологій, то як і з прикладом попередніх авторів, В. Трепак лише натякає на так звану кримінологічну статистику та її методи (статистичне спостереження; статистичне зведення та групування; отримання абсолютних, відносних та середньообчислених узагальнених даних; опрацювання показників; якісний аналіз), завдяки яким стає можливим виявлення масштабів корупції, оцінка ефективності боротьби з нею, тенденції змін, успіхи та невдачі боротьби з корупцією тощо.

На думку автора, основна увага в сфері протидії корупції «має бути зосереджена на запобіганні корупції шляхом усунення можливостей (умов) для вчинення корупційних діянь» (Трепак, 2020, с. 287-289) у таких способах як забезпечення якості законодавства; розвиток електронного декларування; пов'язаний з цим контроль за незаконним збагаченням; продовження люстрації з дотриманням конституційних принципів і прав людини.

Продовженням теми попередження / протидії корупції на регіональному рівні є дослідження О. Новікова. Автором запропоновано власне визначення феномену корупції (Новіков, 2020, с. 50) та терміну «протидія корупції» як діяльності по зменшенню «можливостей для корумпованості суспільних відносин» та визначено фактори її ефективності: «наявність політичної волі держави щодо протидії корупції; вибір напрямів протидії корупції; стан антикорупційного законодавства; наявність сильної незалежної судової влади та компетентних правоохоронних органів; стан економіки; ступінь корумпованості; наявність науково обґрунтованих програм протидії найбільш небезпечним та найбільш поширеним корупційним проявам; рівень розвитку демократичних інститутів суспільства тощо» (Новіков, 2020, с. 53).

Наступна робота Д. Костенко присвячена історії становлення та розвитку системи запобігання корупції в Україні. Автором виділено 6 етапів розвитку системи попередження / протидії корупції в Україні: I етап (Становлення); II етап (Формування основних засад попередження / протидії корупції); III етап (Псевдопротидія корупції); IV етап (Посилення попередження / протидії корупції); V етап (Законодавче реформування); VI етап (Комплексне реформування антикорупційного законодавства) (Д. В. Костенко, 2020, с. 22-23).

Автор зачіпає дотичну нашому дослідження проблему інформаційного забезпечення боротьби з корупцією, яку визначено як «автоматизовану систему інформації і методів її опрацювання, що дає можливість виявлення реального стану корупційних проявів в Україні або в конкретному регіоні держави, а також визначення причин та умов, які стимулюють прояви цього різновиду правопорушення, з метою визначити їхні тенденції для того, щоб ефективно провести необхідні заходи по попередженню чи боротьбі з корупцією» (Д. В. Костенко, 2020, с. 117). Д. Костенко запропонував модель оптимізації системи попередження корупції в Україні «шляхом постійного моніторингу системи державного менеджменту на наявність проявів корупції», що складається з аналізу рівня кадрової безпеки; оцінки рівня негативного впливу інших чинників; виявлення їх причин; планування безпекових заходів;

планування політики кадрової безпеки; реалізація цих заходів; оцінка реалізації запланованих заходів (Д. В. Костенко, 2020, с. 156-157).

На думку автора, мета антикорупційної діяльності може бути досягнута за рахунок упровадження новітніх превентивних антикорупційних механізмів, а саме: декларування майнового стану посадовців, перевірки їхньої доброчесності, моніторингу її способу життя, запобігання та врегулювання конфлікту інтересів тощо.

Актуальною виявилося дослідження А. Приходько щодо адміністративно-правового забезпечення попередження / протидії корупції в Україні за умов євроінтеграції. Так, за результатами дослідження (Приходько, 2020, с. 83-84), сучасні наукові погляди на корупцію поділяються на 5 напрямків:

1. Напрям дослідження інтеграції міжнародних і національних механізмів кваліфікації, виявлення та протидії корупції, що узагальнює поняття «корупція», стандарти діяльності посадових осіб, регламентів для управлінських структур тощо.

2. Напрям дослідження детермінації інституціональних характеристик корупції, що передбачає поєднання політичних, соціально-економічних, соцієтальних і юридичних складників.

3. Напрям дослідження корупції в контексті концепції належного врядування, в якому досліджується вплив корупції на ефективність державного управління та здатність державної системи протидіяти корупції.

4. Напрям дослідження корупції в контексті дотримання прав і свобод людини в системі публічного управління.

5. Напрям дослідження корупції в контексті організованого управління (Приходько, 2020, с. 84). Саме в цьому напрямі «вірним шляхом … слід вважати перехід до вироблення та прийняття урядових рішень, які базуються суто на цифрових технологіях з одночасним забезпеченням ефективного залучення до цього процесу громадськості; реалізацію комплексного та індивідуалізованого підходу до надання державних послуг користувачам з одночасним усуненням їх

від безпосереднього контакту з державними службовцями (деперсоніфікація)» (Приходько, 2020, с. 88).

Неможливо оминути дослідження О. Лозинського щодо психологічних чинників інтолератного ставлення громадян до корупції. Робота кардинально відрізняється від попередніх робіт, адже автор зосереджує увагу на психологічних особливостях ставлення особистості до корупційної соціальної реальності: корупційній організаційній субкультурі, самототалітаризмі, амбівалентності до корупційних ситуацій, антикорупційної спроможності, радикалізмі до корупції. На думку автора, існує два основних підходи до розуміння сутності корупції, а саме: 1) корупція як економічне явище (хабарництво та розкрадання ресурсів); 2) корупція як зловживання (перевищення) владою. Кожний з цих підходів доповнює один одного: «економічні мотиви більше проявляються на рівні «низової» корупції, а політичні мотиви актуалізуються на рівні «верховної» корупції» (Лозинський, 2021, с. 28).

Згідно з автором (Лозинський, 2021, с. 56), корупційна організаційна субкультура складається з таких елементів:

1. Посадові злочинці як носії корупційної субкультури, так би мовити інсайдери злочинного світу. В тій або іншій організації кількість посадових злочинців може варіюватися в залежності від її розміру, які можуть створювати свої кримінальні кліки або команди.

2. Корупційна гра – кожний член корупційної кліки веде подвійне життя: офіційно декларує соціально прийнятні цілі, на публіці грають соціально прийнятні ролі (директора, керівника, секретаря, спеціаліста тощо). За лаштунками ці злочинці використовують посадові, статусні можливості для корупційних зловживань. Мабуть для заспокоєння власної совісті, учасники таких ігор доволі часто звертаються до евфемістичних висловів для пом’якшення опису своєї діяльності: не хабар, а виробничі витрати, не підробка, а налаштування тощо.

3. Залучення додаткового персоналу в корупційну діяльність, що висловив свою лояльність до керівників злочинного угрупування (Лозинський, 2021, с. 57).

4. Засоби впливу на виконавців корупційних дій – використання авторитарного стилю управління, створення бюрократичних бар'єрів між керівником та персоналом та/або клієнтами, демонстративний фаворитизм. Серед стимулів впливу використовують: «а) для обраних і лояльних – підкуп, кар'єрне зростання, публічна похвала, покращення умов праці; б) для пересічних – маніпулятивне переконування (обман), психологічне приниження, шантаж; в) для нелояльних (які виявили спротив) – покарання, показові звільнення, переслідування» (Лозинський, 2021, с. 57).

5. Результатом формування особистості в умовах корупційного середовища стає виникнення низки глибоких психологічних і поведінкових девіацій. Зокрема, йдеться про явище самототалітаризму, що проявляється в приниженні власної гідності, втраті самоповаги та безумовному прийнятті домінування керівника, залученого до корупційних практик, із повною передачею йому права ухвалювати рішення. Відбувається також ідеалізація та міфологізація владних структур: працівники починають приписувати фігурантам корупції риси, що викликають або некритичне захоплення, або пригніченість і тривожність. Іншим наслідком є розвиток автоцензури – відмова від артикулювання власної позиції у відповідь на неправомірні вимоги, а натомість демонстративне схвалення дій керівника та його оточення. Все це підкріплюється гіперлояльністю, коли окремі індивіди намагаються перевершити одне одного в прагненні догодити лідерові, незважаючи на очевидну неетичність або протиправність його поведінки.

Як зазначає автор, у суспільстві, де корупція набула системного характеру, протиправні дії нерідко мають вигляд прихованої соціальної взаємодії між представниками вищих політичних та соціальних еліт. Такі корупційні схеми здебільшого залишаються поза полем публічного виявлення, що робить їх практично невидимими для громадськості та недосвідчених зовнішніх

спостерігачів, які не мають доступу до внутрішніх механізмів владних відносин (Лозинський, 2021, с. 58).

Для звичайного спостерігача (інспектора, клієнта) нічого особливого не відбувається в роботі установи або поведінці її співробітників, всі начебто працюють в межах посадових інструкцій, у звітній документації також «все в ажурі». Адже корупціонери намагаються не залишати явних чи документальних слідів злочину. А усні свідчення співробітників таких установ не можуть надати достатніх доказів наявності в установі корумпованої групи посадових злочинців. Саме тому корупційні злочини є одними з найважчих для розслідування. Корупція має свої прояви у поведінці суб'єктів корупційних дій, а саме демонстративному споживанні та аморальних, протиправних, насильницьких діях.

Корумповані посадові особи безпосередньо рідко беруть участь у злочинних діях, вони приймають рішення, виконувати які доводиться співучасникам (заступникам, підлеглим). Тому «довести провину організаторів є не простою справою, вони часто залишаються безкарними» (Лозинський, 2021, с. 60).

Нарешті одним з останніх у вітчизняному науковому просторі ґрунтовних досліджень феномену корупції є робота М. Кікалішвілі. Авторка аналізує різницю між такими термінами як «запобігання», «боротьба» та «протидія» по відношенню до феномену корупції. В цій роботі для всієї соціальної діяльності, що спрямовано на подолання корупції, використовується термін «протидія корупційній злочинності», який інакше можна виразити словосполученням «антикорупційна діяльність» (Кікалішвілі, 2021, с. 198-199).

Дослідниця надає розгалужену класифікацію заходів попередження / протидії корупції за такими критеріями як: зміст та мета застосування, масштаби застосування, термін дії та нагальність застосування, метод впливу, час їх здійснення, характер вчинюваних заходів, а також авторські системи заходів. Окремо нею досліджується такі теми як комплаєнс-політика, журналістські розслідування та, що дуже тішить, застосування новітніх інформаційних

технологій та інформаційно-аналітичного забезпечення в сфері запобігання та протидії корупції.

В межах цього розглянуто так звану корпоративну корупцію або корпоративне шахрайство, особливо махінації в сфері тендерних закупівель. Як зазначає авторка, «інформація та новітні технології для сучасної боротьби із злочинністю набувають все більшого значення. Інформаційно-аналітична діяльність вбачається важливим складником антикорупційної політики» (Кікалішвілі, 2021, с. 391).

Однією з рекомендацій авторки (Кікалішвілі, 2021, с. 350) є пропозиція активного залучення до роботи правоохоронних органів під час розробки справ корупційного характеру фахівців-аналітиків. Завдяки тому, що аналітики здійснюють попередню обробку даних про злочини, працівники правоохоронних органів отримують у своє розпорядження вже підготовлений оперативно-аналітичний продукт, а не лише сирі масиви первинної інформації. В цілому, робота виконана на високому теоретичного рівні в сфері правознавства, а точніше, кримінального права та кримінології. Незважаючи на це, в роботі недостатньо приділено уваги саме нашому предмету дослідження.

У межах вивчення корупції як загального суспільного явища особливої уваги заслуговують дослідження, що розглядають фінансову злочинність не як ізольований феномен, а як інтегральну складову глобальних соціально-економічних процесів. Прикладом такої роботи є монографія під редакцією М. Акім (*Economic and Financial Crime, Sustainability and Good Governance*, 2023), у якій здійснено спробу комплексного аналізу найбільш поширених форм економічної злочинності сучасності. Корупція в цьому контексті розглядається поруч із корпоративними шахрайствами, податковими махінаціями, діяльністю тіньової економіки, відмиванням коштів, кіберзлочинністю та шахрайствами у сфері криптовалют. Автори демонструють, що всі ці форми економічної девіації мають спільний підґрунтя – ослаблення механізмів належного врядування та ерозію базових принципів прозорості й підзвітності.

Особливістю даної роботи є акцент на взаємозв'язку між поширенням фінансової злочинності та стійкістю суспільного розвитку. Зокрема, підкреслюється, що економічна злочинність прямо впливає на обсяг і якість державних послуг, знижує доходи державного бюджету, підриває стабільність фінансово-банківських установ, обмежує можливості для сталого бізнес-розвитку, а також поглиблює бідність і соціальну нерівність. Тим самим автори демонструють, що корупція й інші форми фінансової злочинності не лише є проявами індивідуальних протиправних практик, а й виступають системними факторами деформації економічних і соціальних структур.

Монографія акцентує увагу на важливості запобіжних стратегій, зокрема інвестицій у програми боротьби з шахрайством, розвиток освіти й підвищення обізнаності громадськості щодо ризиків фінансової злочинності. Пропонується бачення, згідно з яким ефективна протидія фінансовим злочинам має спиратися не лише на жорсткі регулятивні заходи, а й на системні реформи врядування, спрямовані на зміцнення прозорості, доброчесності та інституційної спроможності.

2. Корупція як протиправне діяння.

Друга група робіт розглядають корупцію як протиправне діяння на робочому місці або шахрайство. Більшість досліджень саме політичної корупції не заходять за межі аналізу нормативних механізмів попередження / протидії цьому явищу. Саме тому, наші подальші наукові пошуки були сфокусовані на більш широкому проблемному колі – шахрайстві (occupational fraud – корпоративному шахрайстві). Зазвичай ця тема дуже популярна серед економічних спеціальностей. Слід зазначити, що українські дослідники в контексті нашої проблематики є лише послідовниками попередніх досліджень закордонних представників, що обумовлено тим, що Україна намагається інтегруватися до міжнародної системи корпоративного управління, а не інакше, а тому на наявність унікальних досліджень в цьому сенсі сподіватися важко.

Взагалі, більшість досліджень (монографій) в сфері шахрайства та корупції як формі шахрайства пов'язані із діяльністю ACFE, узагальненої в роботах

Дж. Уелса (Wells, 2014), (Wells, 2017) та (Wells, 2018). До цього переліку можна додати монографічні дослідження (*Machine Learning Applications for Accounting Disclosure and Fraud Detection*, 2021), (*Fraud and Corruption. Major Types, Prevention, and Control*, 2018), (Gottschalk, 2018), (Baesens, Vlasselaer, & Verbeke, 2015), (Vona, 2017). Не зважаючи на яскраві назви, зазначені роботи мають описовий та загально-теоретичний характер, частина матеріалу подається у форматі навчальних посібників, оскільки загальною метою розробки яких є методологічне та методичне забезпечення центру сертифікації фахівців (бухгалтерів, слідчих, судових експертів, аудиторів) в сфері протидії (виявлення) шахрайства, яка є достатньо затребуваною в умовах взаємодії із транснаціональними корпораціями.

Одним з ґрунтовних досліджень на цьому тлі в Україні можна вважати роботу Ю. Хамиги, об'єктом якого стало фінансове шахрайство. «Шахраями називали скритних і нечесних у своїх вчинках людей, хитрюг, махлярів, крутіїв, дурисвітів, ошуканців, пройдисвітів, шельм» (Хамига, 2020, с. 32). А «слово «шахрайство» має спільне коріння зі словом «шахер-махер», що означає «шахрайську операцію; нечесне поводження, гешефт, аферу, махінацію» (*Новий тлумачний словник української мови : в 4 томах*, 2000, с. 862). У науковому обігу можна зустріти синоніми шахрайства, а саме: афера («ризикова справа, здійснювана з метою наживи; шахрайство» (*Великий тлумачний словник сучасної української мови*, 2007, с. 47)) і махінація («несумлінний, нечесний спосіб, витівка, хитрість для досягнення чого-небудь; шахрайство» (*Великий тлумачний словник сучасної української мови*, 2007, с. 653)).

Поряд із цим автор окремо досліджує феномен шахрайства з фінансовими ресурсами держави, що підпадає під визначення змісту корупції. На думку автора, шахрайство з фінансовими ресурсами держави – це сукупність «економічних відносин між юридичними чи фізичними особами та державою в процесі формування, розподілу і використання її фінансових ресурсів, які реалізуються шляхом обману або зловживання довірою чи службовим становищем з метою отримання економічної або/та іншої вигоди (особистої,

корпоративної чи на користь третіх осіб), і призводять до втрати (зменшення, недоотримання) державних ресурсів внаслідок незаконного їх використання» (Хамига, 2020, с. 9).

Серед основних переваг дослідження є представлена автором типологізація способів та інструментів фінансового шахрайства, згідно з якою корупція є однією з форм шахрайства. Під корупцією (і хабарництвом) автор розуміє «не лише їхні зовнішні прояви, але і різновиди внутрішньої корупції у компанії, до яких відносять: комерційний підкуп; несанкціоновані грошові винагороди; «відкати» при розрахунках; спеціальне завищення або заниження ціни за домовленістю тощо» (Климко & Мельник, 2015, с. 188).

В чому ж цінність даного підходу для нашого дослідження? Основною перешкодою в ефективному попередженні та протидії як шахрайству загалом, так і корупційним зловживанням зокрема, залишається проблема їх своєчасної ідентифікації. Як зауважує Н. Ковтун, таку ідентифікацію доцільно здійснювати шляхом інтегрованого застосування математичних, аналітичних і психофізіологічних методів, що, окрім фіксації фактів, дозволяє прогнозувати ймовірні випадки порушень у майбутньому (Ковтун, 2011, с. 14). Вчений рекомендує починати з використання базових математичних алгоритмів, спрямованих на виявлення статистичних відхилень у цифрових рядах емпіричних даних від очікуваних еталонів, що може слугувати індикатором для подальшого цільового аналізу (Ковтун, 2011, с. 12). Доповненням до таких підходів можуть слугувати спеціально адаптовані психологічні тести, які застосовуються в рамках внутрішніх розслідувань, контрольних перевірок або зовнішніх аудитів. В той же час, як підкреслює Ю. Хамига, ефективність таких інструментів значно зростає саме в організаціях із високою інтенсивністю операцій, де накопичуються значні обсяги даних, що відкривають можливість для комплексного аналітичного скринінгу.

Важливу роль у виявленні та прогнозуванні шахрайських і корупційних дій відіграють аналітичні методи дослідження, зокрема методи пов’язаних порівнянь, розрахункових і скорегованих показників, аналізу стереотипних

патернів тощо. Їх ефективність значно зростає за умов інтеграції з комп'ютерними технологіями, що дає змогу автоматизувати процес пошуку аномалій та використовувати додаткові масиви даних. Такий підхід відкриває можливості для застосування сучасних статистичних методів, зокрема аналізу викидів, виявлення нетипових значень і незвичайних залежностей, що істотно підвищує точність оцінювання ризиків і своєчасність реагування. На думку фахівців, «більшість шахрайських махінацій можна виявити, застосовуючи саме автоматизовані аналітичні методи роботи з інформацією» (Ковтун, 2011, с. 12).

Доповнюючим засобом ідентифікації шахрайства та корупції слугують психофізіологічні методи, які ґрунтуються на твердженні, що шахрая «більшою мірою можуть викрити не стільки проникливі слідчі дії чи модернізовані прилади, скільки його власний страх, який викриває обман» (Ковтун, 2011, с. 14).

Автор стверджує, що «в сучасних умовах двоякий вплив на розвиток суспільно-економічних процесів здійснюють цифрові технології, які сьогодні досить стрімко розвиваються і одночасно можуть бути як загрозою для організації, так і інструментом для її захисту» (Хамига, 2020, с. 68). І слушно констатує: «коли йдеться про застосування передових технологій для виявлення шахрайства і протидії йому (наприклад, аналітика даних, тестування транзакцій, моніторинг комунікацій тощо), українські організації у цьому плані значно відстають від решти країн світу» (Хамига, 2020, с. 69). В роботі приділено достатньо уваги способам запобігання, виявлення та протидії шахрайським діям саме у вітчизняній практиці.

Окремий підрозділ дисертаційного дослідження присвячено шахрайству з фінансовими ресурсами держави, яке можна класифікувати за способом реалізації шахрайських схем (дій). У сучасній Україні найбільш поширеними видами шахрайства з фінансовими ресурсами держави, на думку Ю. Хамиги, є: «нецільове використання бюджетних коштів; ухилення від сплати податків; шахрайство у сфері державних закупівель; фальсифікація фінансової звітності; незаконне привласнення активів; корупція; хабарництво та отримання неправомірної вигоди» (Хамига, 2020, с. 112).

У межах підходу, що розглядає корупцію як протиправне діяння на робочому місці, особливої уваги заслуговують дослідження, що фокусуються на психологічних, етичних та соціальних механізмах формування девіантної поведінки. Одним із таких комплексних досліджень є колективна монографія (*Financial Crimes: Psychological, Technological, and Ethical Issues*, 2016). У цьому виданні корупція, шахрайство, ухилення від сплати податків, відмивання грошей та кіберзлочинність аналізуються переважно крізь призму індивідуальної та організаційної поведінки. Значна увага приділена психологічним профілям білих комірців, когнітивним чинникам вразливості жертв, а також специфічним етичним дилемам, які виникають у процесі здійснення фінансових злочинів.

Монографія також пропонує розгляд корупційної та шахрайської поведінки у зв'язку з соціалізацією всередині організаційних структур, де девіантні норми та практика тиску на співробітників можуть сприяти розвитку системного порушення закону. Особливо цікавим є акцент на необхідності змінити не лише правову базу, але й самі підходи до виховання етичної відповідальності серед управлінців та працівників через впровадження критичного аналізу кейсів у навчальні програми. Таким чином, проблема шахрайства розглядається не ізольовано, а в широкому контексті організаційної культури, моральних дилем і технологічних викликів.

Автори акцентують увагу на тому, що незважаючи на численні спроби розробити предиктивні моделі поведінки фінансових злочинців, сучасний стан досліджень не дозволяє будувати однозначні прогностичні конструкції. Однак висновки авторів, базовані на психодинамічних і когнітивних підходах, сприяють розвитку профілактичних стратегій у сфері корпоративної безпеки та удосконаленню методик оцінювання ризиків у фінансовій діяльності.

Продовженням цього напряму можна вважати дослідження, що дозволяють поглиблено зрозуміти мотиваційні стратегії та способи самовиправдання осіб, які вчинили службові правопорушення. Однією з таких праць є монографія Д. Голдстроу-Вайт (Goldstraw-White, 2012), у якій проаналізовано особисті виправдання або раціоналізації («accounts») біло-

комірцевих злочинців щодо вчинених ними діянь. Авторка акцентує увагу на тому, як через формулювання виправдань і вибачень правопорушники намагаються зберегти свій позитивний імідж, зменшити моральний осуд або навіть обґрунтувати свої дії як соціально припустимі.

Робота зосереджена на емпіричному аналізі інтерв'ю з особами, засудженими за службові злочини, і пропонує оригінальну типологію ставлення до вини, яка відображає як юридичну поведінку правопорушників (зокрема, вибір процесуальних стратегій у суді), так і внутрішні моральні оцінки власних вчинків. Авторка також розглядає різноманітні сценарії самовиправдання, що варіюються залежно від соціальної ролі правопорушника, специфіки злочинної ситуації, статі правопорушника та оцінки наслідків скоєного для власного життя та репутації.

В цілому робота намагається пояснити те, як службові правопорушники за допомогою інтерпретацій і пояснень конструюють альтернативні образи своєї поведінки, легітимізуючи або мінімізуючи власну кримінальну відповідальність, що дозволяє зрозуміти логіку діяльності як звичайних шахраїв, так і корупціонерів.

3. Корупція як аномалія.

Останній блок публікацій, що має безпосереднє відношення до предмету нашого дослідження, це роботи, в яких корупція розуміється як певна статистична аномалія – тобто розробок у просторі математики, інформаційних технологій, в тому числі, роботи присвячені використанню різного роду індикаторів корупції, проведенні статистичних процедур для перевірки гіпотез та так званий економетричний підхід.

Перша з них датується 2016 роком і присвячена дослідженню електоральної поведінки громадян (і, частково, організаторів виборів) у країнах постсоціалістичного простору, а точніше характеристик електоральної поведінки, що виявляються в даних електоральної статистики. Метою дослідження було пошук відповіді на питання, чи існує «норма» для електоральної поведінки, яку можна виділити з агрегованих даних електоральної

статистики (і якщо так, яка вона), і чи існують «електоральні аномалії», відхилення від норми, які можна пов’язати з фальсифікацією результатів голосування (і якщо так, то які їх властивості) (Кудінов & Яцина, 2020).

Емпіричну базу даного дослідження склали дані електоральної статистики про результати голосування для 78 випадків загальнонаціональних виборів (президент та парламент) у 14 країнах постсоціалістичного простору, зібраної на нижчому рівні агрегації (дільниця для голосування). До досліджуваних країн увійшли колишні республіки СРСР – Вірменія, Грузія; Україна, Молдова; Литва, Латвія, Естонія – та колишні країни «народної демократії» – Болгарія, Угорщина, Польща, Румунія, Чехія, Словаччина, Албанія. Хронологічне охоплення більшості країн – з початку чи середини 2000-х років XIX століття до сьогодні. Вибір автором цих країн було обґрунтовано досить близькими для порівняння з загального історичного і культурного контексту і практично одноразового початку формування інститутів електоральної демократії. Крім того, ці країни використовують досить близькі за дизайном електоральні системи як на президентських, так і парламентських виборах. З іншого боку, ці країни мають різну репутацію у розрізі якості демократичних інститутів, що мало надати достатню кількість даних як для виявлення якості нормальних, демократичних виборів, так і властивостей електоральних аномалій, які можуть бути пов'язані з фальсифікаціями результатів голосування (Кудінов & Яцина, 2020).

Перевагою дослідження є той факт, що в ньому вперше широкий набір методів вивчення електоральної статистики був застосований до даних з великої кількості порівняних країн постсоціалістичного простору, багато з яких раніше не вивчалися або вивчалися лише фрагментарно. Розгляд великої кількості випадків в електоральній криміналістиці є рідкісним явищем – звичайні публікації обмежуються кількома країнами, що ускладнює формування емпіричного уявлення про наявність універсальних рис електоральної статистики та, у разі їх наявності, їхньої сутності. Ключові теоретичні положення даної роботи ми розглянемо у третьому розділі.

Окремою складовою цього напряму робіт є роботи в сфері інформаційних технологій. Наприклад, є робота (Яцина & Кудінов, 2022), в якій представлені результати досліджень внутрішніх інсайдерських загроз, де стандартні технічні засоби не працюють. Під інсайдерськими загрозами розуміються «шкідливі для організації активності, які походять від співробітників всередині організації (периметру захисту), зокрема – від чинних працівників, колишніх працівників, підрядників, ділових партнерів і навіть завербованих працівників або працівників, які спеціально впроваджені в організацію, які мають доступ до конфіденційної інформації за своїми посадовими обов'язками і які мають уявлення про систему управління інформаційною безпекою організації» (Кудінов & Яцина, 2022). Виходячи з цього розробляються методи виявлення ознак інсайдерської активності в умовах постійного накопичення і збільшення даних про взаємодію великої кількості користувачів зі сховищами даних, гетерогенності та поповнюваності даних та обмеження часу обробки даних та створюються системно-технічні та архітектурні рішення для підтримки профільної діяльності оперативних працівників служб безпеки.

Для створення подібних технологічних рішень використовуються методи дискретної математики, статистичного аналізу даних та машинного навчання, інтелектуального аналізу даних, теорії обчислювальних систем та теорії алгоритмів. На відміну від традиційних методів боротьби з шахрайством та крадіжкою інформації, ці рішення орієнтовані на те, що інсайдери «розчиняють» свою незаконну діяльність у потоці щоденних легітимних робочих процедур, що виконуються ними, а звичайні технічні засоби захисту не «бачать» загроз у їхньої діяльності. При цьому ті, хто неодноразово і цілеспрямовано викрадають або фальсифікують дані в інформаційних системах (наприклад, реєстрах), демонструють разючу спритність, найчастіше в основі своїх дій використовуючи легальні процедури, процеси, доступи, надані їм по службі (не рідко використовуючи у своїх цілях і безтурботність колег). Такі дії можуть довго залишатися непоміченими. Саме тому розробляються методи аналітичної оцінки поведінкової діяльності користувачів і персоналу, за допомогою яких можна

обробляти великі обсяги релевантних оперативних даних в обмеженому часовому режимі, а також аналізувати ознаки зловмисної інсайдерської діяльності в поведінці – порушення трудової дисципліни, надмірної кількості отриманих кредитів, конфліктності, неспровокованих відхилень від регламентних процедур тощо, в тому числі корупції.

Розглядаючи корупцію як аномалію, варто звернути увагу на сучасні дослідження, що аналізують виклики використання аналітико-статистичних технологій у сфері кримінального правосуддя. Одним із таких досліджень є монографія Р. Беркса (Berk, 2019), присвячена аналізу алгоритмічних ризиків у процесі прогнозування поведінки правопорушників. Берк показує, що впровадження систем прогнозування рецидиву, заснованих на машинному навчанні, хоча й спрямоване на підвищення точності кримінально-правових рішень, нерідко супроводжується новими формами викривлення справедливості через проблему упередженості даних, політичний тиск і складність визначення критеріїв “справедливого” прогнозу.

Особливий акцент у праці зроблено на тому, що процеси машинного прогнозування не є нейтральними – вони відображають попередні соціальні нерівності, а іноді й поглиблюють їх. Такі технології можуть бути використані як інструмент раціоналізації політичних чи адміністративних рішень, що створює ризик перетворення кримінального правосуддя на механізм закріплення існуючих структурних дисбалансів. При цьому Р. Берк наголошує: справжнє поліпшення прогнозної аналітики можливе лише за умови повної прозорості алгоритмів, чіткої оцінки компромісів між різними критеріями справедливості й активного залучення громадськості до обговорення принципів розробки й використання таких інструментів.

Отже, за результатами аналізу стану наукової розробки проблеми інноваційних аналітико-статистичних технологій попередження корупції в державі було визначено, що ця проблема набуває дедалі більшого значення саме в умовах швидкого розвитку інформаційних технологій, коли те, що ще десять років тому вважалося новацією, сьогодні сприймається як буденність. Тому

актуальність наукового пошуку зміщується в бік адаптації новітніх технологій, включно з алгоритмами машинного навчання, автоматизованим аналізом даних, інтелектуальними системами, а також їхнім застосуванням у контексті цифрового врядування.

Більшість існуючих досліджень умовно можна поділити на три групи: ті, що аналізують корупцію як загальний соціальний феномен; ті, що досліджують її як шахрайство або порушення на робочому місці; і ті, що підходять до цього явища як до статистичної аномалії, котра може бути виявлена за допомогою сучасних інформаційних і математичних інструментів. Таке розділення дозволило побачити багатопластовість досліджуваного питання й зрозуміти, що жоден із цих підходів не є вичерпним.

Визначено, що у вітчизняних дослідженнях акцент поки що робиться переважно на нормативно-правовій площині або на загальних характеристиках явища, тоді як власне технологічні рішення залишаються поза увагою.

Окремо варто підкреслити, що дослідження, присвячені кримінологічній ідентифікації корупційних схем, вказують на значні можливості, які відкриває впровадження аналітико-статистичних інструментів у розслідувальну та превентивну діяльність. Проте навіть у кращих зразках літератури йдеться переважно про застосування класичної кримінологічної статистики, тоді як інноваційні рішення на основі алгоритмів прогнозування, аналізу аномалій, обробки великих масивів даних або поведінкових моделей ще не стали повноцінною частиною наукової парадигми. Це створює додатковий простір для майбутніх досліджень, які могли б адаптувати сучасні досягнення інформаційних наук до потреб боротьби з корупцією.

Загалом наукова розробка теми інноваційних аналітико-статистичних технологій у сфері попередження / протидії корупції наразі перебуває на етапі становлення: ми бачимо значні теоретичні напрацювання в сфері опису явища, але практичні технологічні рішення досі залишаються розрізненими й фрагментарними. Це створює як виклик, так і можливість – шанс побудувати нові наукові моделі, що інтегрують найсучасніші інформаційно-аналітичні

розробки у сферу державного управління, забезпечуючи цим новий рівень якості антикорупційної політики.

1.3. Методологія дослідження проблеми інноваційних аналітико-статистичних технологій попередження корупції в державі

Методологія дослідження інноваційних аналітико-статистичних технологій попередження корупції в державі визначається складністю об'єкта і багатовимірністю предмета, що вимагає інтеграції загальнонаукових, спеціальних і прикладних підходів. Наше дослідження передбачає не лише опис властивостей технологічних рішень, а насамперед виявлення умов, за яких ці рішення можуть реально змінювати правила гри в управлінні публічними ресурсами, знижуючи простір для зловживань і порушень.

Побудова такої методології зумовлена потребою у системному дослідженні, яке поєднує кілька рівнів аналізу: філософсько-онтологічний (природа корупції як соціального явища), інституційний (роль держави як простору як її генерації, так і протидії), технологічний (характеристики систем і програм), емпіричний (випадки, де такі технології були або не були ефективними), і, зрештою, прикладний – тобто моделювання можливостей їх застосування в Україні.

1. Принципи дослідження.

У процесі дослідження нами дотримано низки базових принципів наукового пізнання, які визначили характер постановки завдань, структуру викладу та логіку емпіричної перевірки. Передусім ідеться про принципи наукової обґрунтованості, об'єктивності, всебічності, історизму, комплексності.

Принцип наукової обґрунтованості полягає в тому, що засоби, методи та рішення, які застосовуються у дослідженні, повинні спиратися на науково перевірені положення та результати практики. Його реалізація передбачає обов'язковий збір, аналіз і огляд актуальної економічної, правової, соціологічної та іншої інформації (Шаган, 2014, с. 67). Він вимагає також урахування закономірностей розвитку досліджуваного об'єкта, контекстних умов і загальних

тенденцій, що робить наукове дослідження не лише достовірним, а й прикладним у прогнозуванні (Росохата, 2012). Це дозволило сформулювати не лише гіпотезу, але й конкретні параметри, за якими можна вимірювати ефективність впровадження інноваційних інструментів попередження корупції (див. підрозділ 2.3, 3.1). Уточнення понять у 1.1 базувалося на критичному аналізі літератури та нормативних джерел, що дало змогу уникнути декларативності і закласти основу для міждисциплінарного підходу.

Принцип об'єктивності означає визнання незалежності предмета дослідження від особистісного сприйняття дослідника. У філософському сенсі об'єктивність трактується як форма існування знання, незалежного від суб'єкта пізнання (Свириденко, 2002, с. 441). У соціально-гуманітарному контексті вона вимагає поваги до істини, а також утримання від тенденційної оцінки явищ (наприклад, корупції) з позицій виключно позитивізму чи моралізму (Волошин, 2013). Принцип орієнтує на зниження рівня упередженості у виборі фактів, інтерпретацій і методів, дозволив відмовитися від нормативного підходу до розуміння технологій як апріорі ефективного антикорупційного інструменту. Як показано в підрозділі 3.3, надмірне захоплення технократичними інтерпретаціями може призвести до легітимації нових форм непрозорості – вже не політичної, а цифрової. Саме тому ми свідомо включили в аналіз критичні позиції щодо використання ШІ в адміністративному управлінні, аналізуючи їх вплив на зниження публічного контролю.

Принцип всебічності означає обов'язкове врахування як внутрішніх, так і зовнішніх зв'язків досліджуваного об'єкта з його оточенням. Він передбачає врахування як об'єктивних чинників (наприклад, інституційної структури, законодавчих змін), так і суб'єктивних (психологічна готовність акторів до реформ), що дозволяє вивчати політичні й управлінські процеси у повноті їхнього змісту (*Методологія наукових досліджень : навчальний посібник для підготовки докторів філософії спеціальностей 161 Хімічні технологія та біоінженерія, 162 Біотехнології та біоінженерія, 163 Біомедична інженерія*, 2021, с. 27). Принцип полягав у залученні не лише технічної чи юридичної

інформації, а й соціального контексту. Ми прагнули вивчити, як аналітичні технології вбудовуються у ширші системи управління, які чинники визначають успішність чи провал їх упровадження. Наприклад, у 3.2 було показано, що технічні можливості самі собою не забезпечують зниження корупційних ризиків, якщо відсутні правові рамки, інституційна підтримка, а також політична воля. Цей принцип також став основою для моделювання загроз, які можуть виникати внаслідок часткової або симулятивної цифровізації управління.

Принцип історизму передбачає аналіз досліджуваного явища в контексті його історичного розвитку та змін. Його застосування дає змогу встановити не лише походження й логіку становлення об’єкта, а й визначити етапи його трансформації та передбачити ймовірні сценарії розвитку. Такий принцип особливо важливий для вивчення процесів цифровізації, які завжди пов’язані з попередніми формами організації управління (Музика, 2012). Згідно з принципом кожне явище слід розглядати в динаміці його розвитку, реалізовано через вивчення еволюції інформаційних систем, аналітичних платформ і принципів державного управління даними. У 2.2 ми простежили трансформацію інформаційних технологій – від допоміжного адміністративного інструменту до систем прийняття рішень, заснованих на прогнозній аналітиці. Окремо було розглянуто український досвід – зокрема, впровадження систем Prozorro, Dozorro, YouControl, які пройшли шлях від експериментальних рішень до державних стандартів.

Принцип комплексності вимагає інтеграції знань з різних наукових дисциплін для повного охоплення об’єкта дослідження. Він орієнтує на поєднання методів політичної науки, публічного управління, економіки, права, соціології, інформатики тощо. Застосування цього принципу дозволяє вийти за межі вузькогалузевого аналізу й побачити аналітико-статистичні технології як явище, що функціонує одночасно в декількох площинах – технічній, нормативній, соціальній (Смирний, 2018, с. 104).

Також принцип дозволив інтегрувати знання з різних дисциплін – від політичної філософії до кібернетики. Особливо це проявилося у залученні

принципів Forensic Social Science (FSS) (Ignatow, 2020), що передбачають послідовне поєднання методів статистичного аналізу з соціологічною і кримінологічною інтерпретацією результатів. Це дозволяє не лише фіксувати факти впровадження аналітичних технологій у сфері антикорупційної політики, але й оцінювати характер їх інтеграції у соціальні структури, рівень ефективності, бар'єри та спротив, що виникають у процесі інституційних змін. Методологічний апарат FSS орієнтує дослідника на критичну рефлексію щодо джерел даних, природи виявлених залежностей та їх потенційних соціальних наслідків. Це дозволяє уникнути механістичного сприйняття статистичних моделей і забезпечує глибше розуміння комплексного характеру корупційних явищ, зумовлених не лише індивідуальними порушеннями, а й системними деформаціями механізмів врядування.

Комплексний характер дослідження також виявляється у зверненні до прикладних інструментів моделювання даних за допомогою мов Python та R.

Зрештою, дотримання усіх зазначених принципів дозволило нам сформувати методологію, що поєднує академічну строгість із прикладною гнучкістю. Ми не лише осмислюємо предмет дослідження на теоретичному рівні, а й створюємо основу для практичного застосування отриманих результатів. Цей підхід відповідає самій логіці новітніх досліджень у сфері політичних наук, де міждисциплінарність, емпірична верифікація та соціальна чутливість до реальних проблем формують новий науковий стандарт.

2. Методологічні підходи.

Методологічна культура дослідження передбачає не лише правильний вибір інструментарію, а й чітке розуміння теоретичної рамки, в якій ці інструменти застосовуються. У нашому випадку йдеться про визначення методологічних підходів, кожен із яких дозволяє висвітлити окрему площину предмета дослідження. Таке поєднання підходів не є механічним, а ґрунтується на логіці зміни масштабу аналізу – від макрорівня (державні інститути, політичні системи) до мікрорівня (алгоритми, моделі, прикладні технології).

Першочерговим в нашому дослідженні є системний підхід. Системний підхід орієнтує дослідників на розгляд досліджуваного об’єкта як цілісної системи, елементи якої взаємопов’язані та взаємозумовлені (Лепський, 2012). Підхід дозволяє розглядати антикорупційну діяльність як елемент більшої політичної та адміністративної системи.

Паралельно з інституційною природою держави, в політологічному дискурсі важливу роль відіграє поняття політичної системи як ширшого контексту, у якому функціонує держава. Держава тут розглядається не як самодостатній актор, а як вузол у складній мережі відносин між суспільством, елітами та міжнародними структурами (Jessop, 2022). Політична система формує рамки для державного управління, визначає домінуючі моделі підзвітності та механізми суспільного контролю. Саме крізь призму якості політичної системи можна оцінювати потенційний ризик корупції: там, де політична система є замкнутою, олігархічною або надто централізованою, корупційні практики стають не винятком, а нормою функціонування (Glazunov, 2015; Глазунов, 2012).

Деякі сучасні дослідження корупції (Fukuyama & Rescanatini, 2021) наголошують на тому, що корупція є результатом не просто зловживань окремих агентів, а відображенням деформованої структури влади, де інтереси еліт переважають над інтересами суспільства. У такому середовищі сама держава стає «корпоративізованою», а політична система – простором боротьби за контроль над ресурсами з використанням нелегітимних або напівлегітимних механізмів.

У нашій роботі системний підхід відіграє подвійну роль. По-перше, як філософська основа системного мислення: ми не аналізуємо окремі технології у відриві, а вивчаємо їх у взаємодії з державними інституціями, громадськими ініціативами та міжнародними стандартами (див. підрозділи 2.2 і 3.2). По-друге, у вузькому сенсі як концепція, що пояснює необхідність узгодженості між різними підсистемами (законодавство, технічна реалізація, професійна етика тощо).

У роботі активно використано також структурно-функціональний підхід. Згідно з підходом, у межах будь-якого системного об’єкта його структурні елементи (компоненти або підсистеми) визначаються не лише за місцем у загальній побудові, а й за виконуваними функціями. Структура системи формується через зв’язки між цими елементами та їхню взаємодію, що забезпечує її цілісність. При цьому кожен елемент здійснює специфічні функції, які в сукупності реалізують загальні функції системи. Важливо, що структура системи розкривається в умовах статики, тобто у фіксованому взаєморозташуванні елементів, тоді як функціональні властивості виявляються у динаміці – у процесі реального функціонування системи (*Методологія наукових досліджень : навчальний посібник для підготовки докторів філософії спеціальностей 161 Хімічні технологія та біоінженерія, 162 Біотехнології та біоінженерія, 163 Біомедична інженерія*, 2021, с. 48).

Підхід дав змогу описати інформаційні системи не лише як набір елементів, а як цілісні утворення з визначеним функціональним призначенням. Як показано в підрозділі 3.1, аналітико-статистичні системи мають власну ієрархію модулів, рівнів обробки даних та типів вихідної інформації. Саме завдяки цьому підходу стало можливим провести чітке розрізнення між системами збору даних, моніторингу, прогнозування та DSS-системами підтримки прийняття рішень. Це дозволило сформулювати типологію технологій та зіставити їх з фазами антикорупційного управління.

Провідне місце в нашому дослідженні посідає інституційний підхід, що передбачає аналіз політичних і правових процесів через призму функціонування інституцій – стабільних норм, структур, організацій, які визначають правила поведінки суб’єктів (Болотіна, Стешенко, & Бородай, 2023). У дослідженні антикорупційних технологій інституційний підхід дозволяє розглядати державу як середовище, в якому формуються й реалізуються інструменти попередження / протидії корупції, з урахуванням динаміки владних повноважень, підзвітності та механізмів контролю.

Як підкреслює С. Ліндер і Б. Пітерс (Linder & Peters, 1990), інституціоналізм пропонує аналіз політичної поведінки як такої, що завжди відбувається всередині інституційного середовища, яке не лише обмежує, а й конститутивно формує політичну дію. У межах антикорупційного дослідження це означає, що будь-які технології – включно з інноваційними аналітико-статистичними – функціонують не у «чистому полі», а в межах нормативних структур, які надають їм або легітимність, або навпаки – формальність, що маскує корупційні практики.

Крім того, погляд на державу як інституційну корпорацію, що управляє суспільним ресурсом, дозволяє глибше осягнути ризики корупційної деформації (Трофименко, 2020). Як і будь-яка корпорація, держава має внутрішню структуру делегування повноважень, централізацію прийняття рішень та складну систему контролю за виконавцями. Проте, на відміну від приватних корпорацій, де механізми нагляду визначені ринковими стимулами, у державі такі механізми значною мірою залежать від політичних процесів та якості інституційної культури. Саме у цій точці виникає головна проблема: коли держава, що мала б діяти як неупереджений арбітр суспільних інтересів, перетворюється на інструмент обслуговування вузькогрупових або приватних інтересів, простір її функціонування стає природним середовищем для корупції.

Таким чином, інституційний підхід дозволяє побачити, що ефективність антикорупційних інструментів залежить не лише від їхньої технічної якості, а й від логіки розподілу влади, процедур прийняття рішень і глибинної культури підзвітності. У підрозділі 2.1 цей підхід дозволив описати державу як форму делегованого управління суспільними ресурсами, де ризик корупційної деформації виникає внаслідок збоїв у механізмах нагляду, підзвітності та публічного контролю.

У нашому дослідженні також застосовано нормативний (управлінський) підхід. Нормативний підхід у політичному дослідженні спирається на концептуальну рамку, що ґрунтується на цінностях, ідеалах та принципах, які вважаються бажаними або належними у певному політичному устрої. Його

мета – не просто описувати те, що є, а формулювати те, що має бути, тобто обґрунтовувати норми, за якими має функціонувати політична спільнота. Як підкреслює Д. Пєтржик-Рівз (Pietrzyk-Reeves, 2017), нормативна політична теорія містить елемент філософського узагальнення та оцінювання, без яких політична аналітика втрачає свою гуманістичну основу. Такий підхід є необхідним, коли йдеться про оцінку політичної справедливості, прав людини, демократичної легітимності чи публічної відповідальності – понять, які не можуть бути зведені до чисто фактичних характеристик.

Загальновизнано, що ключовим чинником формування простору корупційних ризиків є якість урядування (Bagenholm, Bauhr, Grimes, & Rothstein, 2021), що характеризує рівень неупередженості, ефективності та підзвітності державних інституцій (Kirby & Wolff, 2021; Rothstein, 2021). Якість врядування визначає не тільки здатність держави забезпечувати публічні послуги, а й рівень довіри громадян, сприйняття легітимності політичної влади та стійкість до зовнішніх і внутрішніх викликів. При низькому рівні навіть найкращі нормативні рамки залишаються на папері, поступаючись місцем практикам фаворитизму, кумівства та патронату.

Концепція якості врядування виходить за межі традиційного уявлення про державу як механізм прийняття рішень. Вона акцентує увагу на тому, яким чином влада реалізує свої повноваження: чи є ця реалізація неупередженою, прозорою, підзвітною громадянам. При низькому рівні якості врядування ухвалення рішень супроводжується високим ступенем дискреції, коли посадові особи мають широкий простір для особистих інтерпретацій і привласнення суспільних ресурсів для приватних цілей (Fukuyama & Rescanatini, 2021). Натомість високий рівень передбачає обмеження дискреції чіткими процедурами, ефективний контроль та наявність реальних санкцій за порушення правил.

В контексті нашого дослідження нормативний підхід полягає у тому, щоб розглядати якість врядування як ключовий чинник ефективності боротьби з корупцією. Як зазначено в підрозділі 2.3, навіть найбільш технологічно

просунуті рішення не можуть бути ефективними у разі низького рівня підзвітності та відповідальності виконавців. Нормативний підхід дозволив осмислити аналітико-статистичні технології не як заміну людському управлінню, а як інструмент, що лише підсилює або, навпаки, послаблює ефект залежно від контексту реалізації. Зокрема, від якості організаційної культури, законодавчих норм та рівня цифрової грамотності.

Поведінковий (біхевіористський) підхід у політичному дослідженні полягає в орієнтації на емпіричне вивчення дій і реакцій індивідів та груп у політичних умовах. Його метою є формулювання гіпотез про політичну поведінку, які піддаються верифікації методами, що відповідають канонам сучасного емпіричного знання. Як зазначає Р. Даль (Dahl, 1961), особливістю поведінкового підходу є зосередження на політичному акторові як індивіду, його мотиваціях, установках, уподобаннях, рішеннях та участі у політичних процесах. Саме індивідуальні дії розглядаються як первинні одиниці аналізу. Методологічно підхід передбачає використання кількісних методів, опитувань, статистичних моделей, що дозволяють вивчати політичні переконання, схеми голосування, рівень участі у виборах, політичну соціалізацію тощо. У такому розумінні, як підкреслює Р. Даль, політична поведінка не є окремим полем дослідження – це радше орієнтація, яка прагне описати всі явища урядування через спостережувану поведінку людей як учасників політичної системи.

Підхід знайшов своє застосування у підрозділах 2.3 та 3.3. В першому випадку він став основою для аналізу поведінки «інсайдерів», в другому – аналізу можливих ризиків цифровізації політичного процесу.

У структурі методологічного забезпечення політичного дослідження часто постає питання: чи доцільно виділяти емпіричний підхід як самостійний, якщо інші підходи – інституційний, нормативний, поведінковий – також можуть передбачати звернення до фактичних даних. Ця проблема не є лише формальною, адже йдеться про розмежування функцій різних типів підходів у дослідницькому процесі. Як свідчить аналіз наукової літератури та практики застосування підходів у політології, теоретико-пояснювальні рамки та

методологічні орієнтації виконують різні ролі, хоч і можуть перетинатися у своїй реалізації.

Так, інституційний, нормативний і поведінковий підходи є насамперед теоретичними або концептуальними орієнтаціями, які задають фокус аналітичного бачення: що вважається значущим у дослідженні, як саме інтерпретуються ключові процеси, що виноситься у центр уваги. Інституційний підхід фокусує дослідження на нормах і структурах, які регламентують політичну поведінку; нормативний – на етичних засадах політичного порядку; поведінковий – на спостережуваних діях акторів. Водночас, кожен з них може застосовуватись як у теоретичному, так і в емпіричному вимірі: наприклад, поведінковий підхід нерідко реалізується через аналіз даних опитувань, а нормативний – через аналіз практик публічного управління щодо дотримання правових стандартів.

Натомість емпіричний підхід не є альтернативним цим теоретичним напрямам – він виконує іншу, прикладну функцію. Це орієнтація дослідження на спостереження, збір, опис та аналіз фактів, незалежно від теоретичної позиції. Іншими словами, емпіричний підхід забезпечує операційну реалізацію дослідницької програми: визначає, які саме джерела даних використовуються (вибірки, кейси, публічні реєстри, поведінкові патерни), яким чином здійснюється вимірювання, за допомогою яких методів – кількісних чи якісних – дані обробляються та інтерпретуються. У цьому розумінні емпіричний підхід є перехресною матрицею, яка може поєднуватись із будь-якою теоретичною основою.

У межах нашого дослідження, наприклад, інституційний підхід дав змогу інтерпретувати державу як простір делегування повноважень і відповідальності (підрозділ 2.1), а емпіричний підхід – дослідити, як це реалізується через конкретні інструменти: систему Prozorro, модулі аналітики, відкриті бази даних, логіку роботи інсайдерів (2.3, 3.1, 3.2). Саме емпіричний підхід дозволив перейти від концептуального осмислення антикорупційної технології до практичного тестування моделей, симуляції сценаріїв і верифікації гіпотези.

Таким чином, емпіричний підхід виконує інструментальну функцію реалізації дослідження, забезпечує його верифікованість, дозволяє перевірити гіпотези та отримати дані, що можуть бути використані для формування висновків і рекомендацій. Незалежно від обраної теоретичної орієнтації, саме емпіричний підхід дає змогу говорити про наукову доказовість отриманих результатів.

3. Методи дослідження.

Саме тут ми переходимо безпосередньо до методів дослідження. Інструментом теоретико-практичного дослідження будь-якого предмету є науковий метод. Метод – це впорядкована діяльність для досягнення певної мети. Тому, науковий метод – це сукупність дій вченого у формі розумових або фізичних операцій, які виконуються ним під час дослідження. Метод ґрунтується на застосуванні певних процедур з метою отримання нових знань. Вибір того чи іншого методу дослідження залежить від властивостей та особливостей об'єкта дослідження, а також метою (потребою, інтересами) дослідження. Тому науковий метод є як результатом наукової діяльності людини, так і засобом для її подальшої роботи (Монастирський, 2014, с. 8).

Методологічна база нашої роботи сформована з урахуванням поєднання загальнонаукових, спеціальних і емпіричних методів. Основу методологічного каркасу становлять загальнонаукові методи, зокрема аналіз, синтез, індукція та дедукція.

Синтез (дослідження шляхом об'єднання елементів, характеристик та параметрів об'єкта в єдину одиницю вищого порядку – сукупність) та аналіз (розподіл цілісного об'єкта на окремі елементи, що може мати місце як в уяві, так і на практиці) (Лісовий, 2001) – застосовано для дослідження інформаційних систем, що створюються в процесі впровадження аналітико-статистичних технологій в діяльності суб'єктів антикорупційної політики.

Індукція (пізнання шляхом сходження від окремих фактів до загальних висновків) та дедукція (формулювання висновків про окремі факти шляхом сходження від загальних характеристик) (Тофтул, 2011) забезпечили можливість

дослідження конкретних програмних застосунків, що дозволяють використати інноваційні технології ідентифікації корупційних схем у найбільш розповсюджених сферах суспільства: державних закупівель, електоральних процесах тощо.

У ході дослідження використано метод аналогії, що дозволив перенести підходи з суміжних галузей – наприклад, управління якістю або виявлення шахрайства у фінансовій сфері – до сфери боротьби з корупцією. Зокрема, в другому розділі ми показали, як системи управління ризиками в бізнесі були адаптовані для публічного управління, створюючи новий клас інформаційних рішень. Метод аналогії дав змогу глибше осмислити, що «аналітико-статистична технологія» – це не окремий прилад чи програмне забезпечення, а модель дії.

Застосування прогностичних методів (зокрема, моделювання й сценарного аналізу) було необхідним для оцінки потенціалу масштабування інноваційних технологій. У підрозділі 3.3 ми описали три сценарії розвитку цифрової антикорупційної інфраструктури в Україні – песимістичний, реалістичний і оптимістичний – використовуючи методи екстраполяції та ризик-аналізу. Такий підхід дозволив не лише інтерпретувати поточні дані, а й створити підґрунтя для стратегічних рекомендацій.

На емпіричному рівні застосовано метод спостереження та контент-аналізу відкритих даних: офіційної документації, діючого законодавства, контенту офіційних веб-сторінок публічних органів влади та виробників спеціалізованого (аналітико-статистичного) програмного забезпечення, особливо тих веб-ресурсів, що безпосередньо акцентують увагу споживачів на можливостях застосування їх інформаційних систем як інструменту попередження корупції, в тому числі аналіз соціальної дійсності, середовища існування корупції та поведінки суб’єктів корупції, аналіз існуючих (задокументованих) прикладів антикорупційних практик, а також матеріали журналістських розслідувань корупції та шахрайства, історії успішного застосування тих або інших інформаційних технологій у антикорупційній діяльності, матеріали міжнародних неурядових організацій тощо.

З праксеологічної точки зору роботу неможливо було провести без застосування такого методу як експеримент. Для ознайомлення з недоліками та перевагами існуючих аналітико-статистичних рішень для попередження / протидії корупції, автором було протестовані більшість із вказаних в дослідженні технічних ноу-хау: починаючи від використання відомого більшості інструменту Microsoft Office Excel, IBM SPSS Statistics і закінчуючи створенням навчальної бази даних для студентів факультету соціології та управління Запорізького національного університету з метою застосування алгоритмів пошуку аномалій засобами R та Python (Кудінов & Яцина, 2024), а також даних, представлених у репозиторіях www.github.com та www.kaggle.com. Залишилися поза увагою ті програмні застосунки, впровадження яких потребує створення штучного середовища, що значно виходить за межі безкоштовного (умовно-безкоштовного) використання інформаційно-обчислювальних ресурсів, а саме застосунки корпоративного рівня від компаній IBM, SAS, SAP, Deloitte, EY, PwC, KPMG тощо.

Нарешті, останнє – сервіси штучного інтелекту. У процесі написання дослідження було свідомо інтегровано елементи використання генеративного штучного інтелекту, зокрема моделі ChatGPT, що відповідає визначеним у Рекомендаціях Міністерства цифрової трансформації України ("Рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в закладах вищої освіти," 2025) принципам етичного та академічно доброчесного застосування таких систем.

Відповідно до запропонованої «шкали прийнятного використання генеративного ШІ», модель не виконувала завдань повністю, натомість використовувалась як допоміжний інструмент. Усі запити були сформульовані з позицій автора дослідження, а кінцевий результат проходив критичне осмислення, перевірку фактів і теоретичне узгодження з першоджерелами.

Найбільшою мірою генеративний ШІ було залучено на етапах попереднього аналізу літератури (наприклад, для коротких узагальнень змісту об’ємних джерел) та кодування. Зокрема, під час розробки Python-скриптів для

збору, обробки відкритих масивів даних ШІ використовувався як засіб дебагінгу й оптимізації (Додаток 5 згаданих Рекомендацій).

Також були реалізовані функції автоматичного стенографування аудіо-, відеозаписів, перекладу фрагментів англомовної літератури, розміщеної у відкритому доступі із застосуванням власноруч розробленим Python застосунком із використанням API OpenAI та AssemblyAI (Yatsyna & Kudinov, 2025). При цьому стенограми або переклад не використовувались як фінальний результат без авторського доопрацювання. Кожен текст було переглянуто, адаптовано до термінологічної бази української науки, а також перевірено на відповідність змісту оригіналу. Таким чином, застосування ШІ не підміняло інтелектуальну діяльність автора дисертації, а стало інструментом оптимізації та підвищення ефективності роботи з великими обсягами інформації.

Таким чином, методологія дослідження інноваційних аналітико-статистичних технологій попередження корупції в державі базується на визнанні багатовимірності предмета та потребі поєднання загальнонаукових, спеціальних і емпіричних методів. Такий підхід дозволив структурувати завдання дослідження, а також забезпечити їх реалізацію у спосіб, що відповідає сучасним стандартам доказової науки. Дотримання принципів наукової обґрунтованості, об’єктивності, історизму, всебічності та комплексності надало дослідженню внутрішньої цілісності. Зазначені принципи було реалізовано через системну інтеграцію з обраними методологічними підходами: системним, інституційним, нормативним, структурно-функціональним, поведінковим та емпіричним. Кожен з них виконував окрему функцію у дослідницькому процесі: від формулювання базових уявлень про природу корупції й держави до осмислення практичної взаємодії технологій з політичними інституціями, публічними акторами та поведінковими патернами.

Висновки до першого розділу

Підсумовуючи результати першого розділу, можемо сформулювати такі положення.

По-перше, поняття «корупція» виходить далеко за межі правового або економічного визначення. Корупція проявляється як складне соціальне, психологічне, культурне й політичне явище, в якому переплітаються індивідуальні мотиви, інституційні практики й системні деформації влади. Проведений аналіз підтвердив, що неможливо дати єдине універсальне визначення цього феномена. Тому його потрібно розглядати як правову девіацію, як соціально-політичний інститут, як культурно-психологічний феномен і як набір групових стратегій.

По-друге, було визначено різницю між поняттями «попередження», «запобігання», «боротьба» та «протидія» корупції. Попередження корупції визначено як систему цілеспрямованих дій, методів, процедур або технологічних рішень, спрямованих на виявлення, нейтралізацію або трансформацію соціальних, управлінських, інституційних і психологічних факторів, які потенційно сприяють корупційній поведінці, ще до того, як така поведінка набуде форми фактичного правопорушення.

По-третє, було розглянуто сутність інноваційних аналітико-статистичних технологій в контексті попередження / протидії корупції. У широкому сенсі це технології, що використовують сучасні методи математичного аналізу, статистики, машинного навчання, нейронних мереж і аналізу великих даних для виявлення аномалій і закономірностей. У вузькому значенні – це інструменти, які дозволяють здійснювати моніторинг і виявлення корупційних ризиків у режимі реального часу. Ці інструменти є фундаментальним компонентом модернізації антикорупційної політики. Вони стають засобом, через який держава і суспільство можуть адаптуватися до викликів цифрової доби.

По-четверте, аналіз наукової розробленості проблеми інноваційних аналітико-статистичних технологій попередження корупції в державі дозволяє охарактеризувати її як науковий напрям, що стрімко розвивається, орієнтований на практичне застосування у сфері контролю якості діяльності органів державної влади та місцевого самоврядування. Разом з тим, слабка розробленість тематики інструментів попередження / протидії корупції в державі із залученням новітніх

інформаційних (в тому числі аналітико-статистичних) технологій у дослідження дозволяє говорити про значний резерв в осмисленні наявного досвіду і адаптації існуючих можливостей до умов існування держави, що змінюється. Вітчизняна наука поки що відстає в практичному застосуванні новітніх технологій, хоча потенціал адаптації закордонного досвіду залишається значним.

Нарешті, п’яте, обґрунтовано методологію дослідження. Методологічна база забезпечила дослідженню внутрішню цілісність, логічну послідовність та практичну релевантність. Поєднання принципів об’єктивності, всебічності, наукової обґрунтованості й історизму з системним, структурно-функціональним, інституційним, нормативним і поведінковим підходами дозволило не лише сформулювати комплексне бачення досліджуваного явища, а й закласти підґрунтя для побудови цілісної аналітичної моделі. Емпіричний і прогностичний компоненти методології – аналіз реальних кейсів, верифікація алгоритмів, моделювання сценаріїв – посилили прикладну цінність дисертаційного дослідження.

Застосований у роботі методологічний комплекс дав змогу розглядати інноваційні аналітико-статистичні технології не як ізольоване технічне явище, а як складову широкого соціально-політичного процесу. Завдяки міждисциплінарному підходу та цифровим інструментам аналізу було забезпечено як теоретичну глибину, так і практичну результативність дослідження, що відкриває можливості для подальшої розробки стратегії цифрової трансформації антикорупційної політики в Україні.

РОЗДІЛ 2
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІННОВАЦІЙНИХ АНАЛІТИКО-СТАТИСТИЧНИХ ТЕХНОЛОГІЙ ПОПЕРЕДЖЕННЯ КОРУПЦІЇ В ДЕРЖАВІ

2.1. Держава як простір виникнення, розвитку і попередження корупції

1. Держава як простір виникнення і розвитку корупції.

Дослідження феномену корупції в межах державного простору неможливе без глибокого осмислення природи самої держави та її функціональної ролі в суспільстві. У класичному дискурсі держава осмислювалася через призму монополії на легітимне насильство (Макс Вебер) або як інструмент панування одного класу над іншим (Карл Маркс). Такі підходи акцентували на примусовому, владному вимірі держави, фокусуючись на її здатності забезпечувати суспільний порядок через апарат примусу. Паралельно правові школи (Ганс Кельзен) визначали державу як правовий порядок, що централізує нормативні приписи та регулює поведінку індивідів у суспільстві.

З розвитком громадянського суспільства, розширенням ідеї прав людини та демократизації політичних процесів з’явилися нові концепції, що розглядали державу не лише як механізм примусу, а як складну політико-правову організацію, яка повинна забезпечувати баланс між суспільною організацією та індивідуальною свободою. Так, сучасне осмислення держави зводиться до кількох консенсусних характеристик: держава має контроль над засобами легітимного насильства, здійснює владу на визначеній території, підтримує суверенітет і має організовану бюрократичну систему управління. Окрім того, вона функціонує на основі правових норм, спираючись на конституційні принципи верховенства права та забезпечення громадянських прав (Бутченко, 2004; Копча, 2020).

Водночас новітні підходи акцентують на тому, що сучасна держава не може розглядатися ізольовано від економічних і соціальних процесів.

Глобалізація, розвиток ринкових відносин, зростання ролі транснаціональних акторів значно ускладнили класичні уявлення про суверенітет і контроль. Х. Пірсон (Копча, 2020) підкреслює, що хоча держави залишаються основними політичними акторами, їхня автономія в управлінні внутрішніми процесами істотно обмежена глобальними економічними та політичними чинниками.

Згідно концепції Б. Джессопа, держава більше не розглядається як єдиний центр прийняття рішень, натомість вона виступає як частина мережевої системи управління, де влада розподіляється між численними акторами. Це мережеве управління (network governance) водночас зменшує прозорість процесів ухвалення рішень і посилює ризики так званої “мережевої корупції”, коли приватні інтереси ховаються під виглядом колективних дій. Політична система, в межах якої функціонує держава, є не просто тлом для її діяльності, а визначальним чинником, який формує можливості або обмеження для розвитку корупційних практик. Держава не існує у вакуумі – вона є частиною складного комплексу відносин між інститутами, елітами та громадянами, де правила гри встановлюються не лише формально через закони, але й неформально через соціальні очікування, баланси сил і традиції політичної поведінки (Jessop, 2022).

Деякі автори (П. Бірнбаум і Б. Баді) визначають державу як інституційну політико-правову машину, яка через мережу функціонерів та адміністративних органів здійснює домінування над громадянським суспільством (Копча, 2020, с. 14-15). Такий підхід поступово створює підґрунтя для сучасного розуміння держави як 1) особливої форми корпоративної організації, де інституційна логіка управління ресурсами, процедурами та владними повноваженнями стає центральною, або 2) організованої структури, що володіє ресурсами, виконує функції управління і має власну систему делегування повноважень (Трофименко, 2020). Саме цей підхід дозволяє краще зрозуміти, чому держава, будучи створеною для забезпечення спільного блага, нерідко стає механізмом концентрації привілеїв в руках вузьких елітарних груп. На відміну від приватних корпорацій, де інтереси власників прямо стимулюють до контролю за

виконавцями, у державі механізми контролю набагато складніші, розмиті між громадянами, політичними представниками та адміністративним апаратом.

У цій логіці особливе місце посідає проблема якості державного управління та політичної системи як індикатора здоров'я або, навпаки, хворобливості "корпоративного організму" держави. Якщо механізми делегування повноважень працюють неефективно, виникають умови для так званої приватизації влади, коли посадові особи починають використовувати державні ресурси для задоволення власних або групових інтересів (Рикова, 2020).

З точки зору класичної теорії, призначення держави полягає у забезпеченні загального блага через легітимне управління суспільством (Терлюк, 2021). Проте на практиці політична система може еволюціонувати таким чином, що держава стає не гарантом суспільного договору, а інструментом захисту приватних інтересів певних груп. В таких умовах відбувається трансформація державних функцій: замість виконання публічних завдань виникає тенденція до використання державних механізмів для особистого збагачення та укріплення влади.

Держава, діючи в політичній системі, де відсутні дієві механізми прозорості та контролю, легко потрапляє у стан конфлікту інтересів, особливо коли сама бере участь у ринкових відносинах через корпоративні механізми (Рикова, 2020). Таким чином, політична система, яка не забезпечує реального розмежування публічного і приватного інтересу, фактично заохочує до структурної корупції: викривляються процедури розподілу ресурсів, приватний інтерес підміняє собою суспільний.

Слабкість політичної системи особливо проявляється через відсутність реальної конкуренції еліт і неспроможність інститутів забезпечувати рівні правила гри. У таких умовах влада концентрується в руках замкнених груп, що використовують державу як інструмент для збереження статус-кво. Саме через ці механізми формується простір для системної, або структурної корупції, де

зловживання владою стають нормою функціонування політичної системи (Скиба, 2014).

Доречною в цьому плані стає концепція захоплення держави (state capture) (Fukuyama & Rescanatini, 2021). Вона описує ситуацію, коли окремі економічні або політичні актори не просто впливають на окремі рішення держави, а системно формують політики, законодавство і правила гри на свою користь. У такій політичній системі держава перестає бути нейтральним арбітром і перетворюється на активного агента приватних інтересів, що поглиблює корупційні ризики.

Не менш важливою є ідея про те, що у деформованій політичній системі навіть механізми громадянської участі – вибори, референдуми, громадські слухання – можуть бути налаштовані для легітимації вже існуючих корупційних порядків. Як показують С. Дітріх і М. Вінтерс (Dietrich & Winters, 2021), у державах із низькою якістю урядування міжнародна допомога, спрямована на підтримку демократичних процесів, може не тільки не зменшувати корупцію, а навпаки – стабілізувати владу корумпованих режимів, які використовують зовнішні ресурси для підтримки лояльності еліт та нейтралізації опозиції.

Таким чином, політична система постає не як нейтральне поле взаємодії інститутів, а як середовище, у якому формується інституційна архітектура можливостей для корупції. Структурна корупція виникає там, де відсутні реальні механізми підзвітності, де громадяни не мають ефективних каналів впливу на владу, а розподіл ресурсів визначається не законами і процедурами, а неформальними угодами між впливовими акторами.

У цьому контексті держава, яка мала б бути втіленням принципу публічного служіння, стає не арбітром у політичній системі, а її активним учасником у боротьбі за ресурси, статус і владу. Це перетворення суттєво змінює природу простору державного управління, трансформуючи його з простору спільного блага у простір системної корупції.

Отже, держава постає як простір, де перетинаються і взаємодіють різноспрямовані сили: інституційні конструкції, економічні стимули, політичні

інтереси та зовнішні впливи. Водночас саме держава, незважаючи на притаманні їй ризики структурної корупції, залишається основним інструментом попередження / протидії цьому явищу.

Продовжуючи аналіз держави як складного середовища виникнення та розвитку корупції, доцільно звернути увагу на іншу її роль – роль активного суб'єкта антикорупційної політики. Саме розуміння функцій сучасної держави у протидії корупції, її інституційної спроможності реалізовувати ефективні механізми стримування і противаг, а також аналіз глобальних стандартів належного врядування дозволяють сформувати цілісне бачення можливостей та обмежень у боротьбі з корупційними практиками.

Ми додержуємося думки В. Трепак про те, що за сучасних умов назріла необхідність нового виваженого підходу до розуміння сутності корупції, метою якого є зменшення рівня корупції в Україні до суспільно прийнятної межі. Суспільно допустимий рівень корупції – це рівень, «за якого корупція: не є масовим явищем і не має системного характеру; не здійснює істотного впливу на політичну, економічну, правову сфери суспільного життя; не є функціональним елементом організованої злочинності та не використовується для прикриття організованої злочинної діяльності; відсутня на найвищому політичному рівні і є малопоширеною у судовій системі та органах правопорядку; характеризується неприйнятним ставленням з боку більшості населення» (Трепак, 2020, с. 39).

2. Класифікація форм і видів корупції в державі.

Оскільки корупція як феномен має багато форм, тому перелік інструментів попередження / протидії цьому явищу постійно перебуває в динамічному розвитку, розділяючись на основні (класичні, стійкі) і вторинні (похідні) інструменти. Поєднання тих або інших інструментів попередження / протидії створює так звані моделі боротьби з корупцією. Так, виділяють чотири основні моделі боротьби з корупцією (Приходько, 2020, с. 115-116):

1) тоталітарна модель – всеосяжний контроль з боку держави за поведінкою посадових осіб і жорстке реагування на будь-які відхилення від прийнятих норм (Китай);

2) авторитарна модель – вибіркова реалізація кримінальної відповідальності щодо посадовців, оскільки посадова особа найвищого рівня отримує правовий імунітет (Білорусь);

3) олігархічна модель – кримінальна відповідальність згідно з клановим підходом «свій – чужий» (Україна до 2022 року);

4) ліберальна модель – повна безвідповідальність, безкарність і вседозволеність, що можливо лише в часи максимальної нестабільності. Прикладами такої нестабільності є революції, війни тощо.

Як зазначає А. Приходько, в нашій країні тривалий час існувала «олігархічна модель боротьби з корупцією, оскільки наміри України щодо викорінення корупції є подвійними. Щонайменше у правлячої еліти та окремих представників політичної волі. З одного боку, з екранів телевізора, друкованих та електронних ЗМІ можновладці активно пропагують нульову толерантність до будь-яких проявів зловживання владою, а з іншого – так само активно використовують її у власних цілях» (Приходько, 2020, с. 116). Такої ж думки була Гельсінська комісія США, яка у своєму звіті «Внутрішній ворог» від 16 жовтня 2017 року заявляла, що «олігархи захопили державу Україна, витіснивши некорумповані політичні партії та змагаючись один з одним, щоб розікрасти українські багатства» (Massaro, 2017, с. 1). Події ж 2022 року безперечно перевели Україну до четвертої моделі корупції, особливості якої науковці будуть досліджувати після закінчення війни.

Від моделей корупції перейдемо до існуючих класифікацій або критеріїв класифікації. О. Новіков пропонує розгорнуту систему класифікації корупційних явищ, спираючись на низку концептуальних критеріїв (Новіков, 2020, с. 51–52). Зокрема, він виокремлює корупцію за типом суспільних відносин, які вона деформує – політичну, економічну, соціальну, соціокультурну тощо. За рівнем суспільної небезпеки корупція може кваліфікуватися як кримінальний злочин, адміністративний проступок або соціально аномальна поведінка. Водночас значення має й сфера поширення: побутова корупція, корупція в приватному та публічному секторах. Також автор розрізняє типи корупції за суб’єктами

вчинення – від посадових осіб, уповноважених на виконання функцій держави, до фізичних осіб і представників приватних юридичних структур. За масштабами вона поділяється на індивідуальну, локальну, регіональну, національну й транснаціональну. Крім того, Новіков враховує ступінь виявленості – прихована, непряма та відкрита корупція – та статус учасників: «дрібна» корупція, притаманна нижчим чиновникам, і «велика» – що охоплює високопосадовців, які вже мають доступ до значних ресурсів і привілеїв.

Корупцію можна класифікувати за характером ситуації, у якій ухвалюється корупційне рішення. Корупційною можна вважати будь-яку ситуацію, у якій ухвалюється рішення, що суперечить закону або моралі суспільства. При цьому дана подія може відбуватися за трьох обставин.

По-перше, в обставинах взаємної згоди сторін, що передбачають одержання незаконного зиску / переваги, наявність яких обидві сторони стараються приховувати, в тому числі і самих таких вчинків.

По-друге, ситуація ухвалення рішення посадовою особою, що здійснюється під тиском (шантаж) другої (зацікавленої) сторони, відбувається переважно з тими посадовцями, яке вже затягнуті до злочинної діяльності, а їх зиск полягає переважно в тому, що їх не виказують, і вони залишаються на своєму робочому місці (Дедекаев, 1998, с. 42).

По-третє, ситуації, коли посадова особа ухвалює відповідні рішення за власним бажанням та за згодою зацікавленої сторони, однак в основі домовленостей між цими сторонами є не отримання взаємної вигоди, а обман зацікавленою стороною посадовця. Взагалі, за таких обставин, жертвою правопорушення стає і сама посадова особа, винність або невинність якої доводиться доводити у судовому порядку.

Існує класифікація корупції, яку умовно поділяють на правопорушення та етичні відхилення. В свою чергу правопорушення поділяються на цивільно-правові делікти, дисциплінарні проступки, адміністративні проступки і правопорушення (Селюченко, Заяць, & Живко, 2010, с. 67).

Дослідники зі Словаччини пропонують типологію корупції за такими критеріями (Sičáková-Beblavá & Beblavý, 2007):

1. За сферою корупції:

– адміністративна;

– політична.

2. За впливом на громадянина:

– велика;

– мала.

3. За рівнем корупційних дій:

– хаотична;

– організована;

– приватна/колективна.

4. За характером виникнення:

– системна;

– індивідуальна.

5. За відносинами між особою, що допускає корупцію, та особою, яка здійснює корупцію:

– внутрішня;

– зовнішня.

6. За формою взаємовідносин:

– примусова (вертикальна);

– добровільна (партнерська);

– у форматі «патрон-клієнт» (політичний клієнтелізм);

– партнерський клієнтелізм.

7. За відношеннями між елітами та масами:

– приватна корупція між неелітами;

– нееліти, що корумпують еліту;

– еліти, що корумпують одна одну;

– еліти, що корумпують нееліти;

8. За мотивацією особи, що здійснює корупційну дію:

– корупція з метою збалансування пропозиції та попиту;
– корупція як мотиваційний елемент;
– корупція з метою зниження витрат;
– корупція з метою забезпечення кримінальних дій.

9. За мотивацією особи, що допускає корупцію:

– корупція з потреби;
– корупція з жадібності.

Останній підхід до класифікації корупції полягає в типізації її найпоширеніших форм прояву. Так, О. Новіков (2020, с. 51) виокремлює серед них такі типові форми, як хабарництво, здирництво, кумівство, протегування, розкрадання державних фондів, незаконне використання бюджетних надходжень, зловживання владними повноваженнями, а також порушення законодавства про вибори, зокрема у фінансуванні виборчих кампаній та організації голосування. Ці форми розглядаються як усталені патерни поведінки, що відображають глибоку вкоріненість корупції в різних сферах функціонування публічного управління.

Крім цього, О. Новіков окреслює низку державних і муніципальних процедур, які найчастіше стають об’єктами корупційних зловживань (Новіков, 2020, с. 135). Серед них – видача ліцензій на підприємницьку діяльність, дозволів на торгівлю та рекламу; маніпуляції під час приватизації державного майна; непрозоре призначення соціальних пільг, інвалідності, санаторного лікування чи регулювання цін на лікарські засоби; втручання в освітній процес, у тому числі в діяльність приймальних комісій; а також численні зловживання у сфері земельних ресурсів – від порушення процедур розпаювання до незаконного виведення земель сільськогосподарського призначення.

Саме в рамках держави можна говорити про достатньо молодий вид корупції як корпоративну корупцію. Саме на рівні корпорацій (холдингів, концернів, корпорацій та навіть держав) набирають поширення не прості фінансові махінації із документацією тощо, а добре розроблені схеми привласнення суспільного багатства чи економічних поборів. Особливу

цікавість корпоративної корупції викликає сфера тендерних закупівель, яким не в змозі завадити навіть такі системи як «Prozorro» (Кікалішвілі, 2021, с. 384). На другому місці у корпоративній корупції знаходяться випадки щодо легалізації доходів, отриманих злочинним шляхом.

Окремим видом корупції вважають політичну корупцію як «деструктивний різновид неформальних інститутів підривного партикулярного характеру, який зумовлює неправомірне використання суб'єктами політичного процесу з корисливих мотивів ресурсів влади в позасуспільних інтересах, приватизацію публічних ресурсів за умов слабкості формальних і конструктивних неформальних інститутів» (Кушнарьов, 2018, с. 90). Як зазначає І. Кушнарьов, вона характеризується:

– «проявом тіньової, неформальної політики; тобто це латентна політика (прихована, непублічна, непрозора частина політичного процесу);

– підривним механізмом, який посягає на стабільність будь-якої інституційної системи;

– загрозою національній безпеці держави, позаяк зумовлює неформальну інституціалізацію, подальшу деградацію державних інститутів;

– практикою, спрямовану на звуження публічного простору, ускладнення циркуляції еліт і монополізацію політичного ринку;

– стійким типом рентозорієнтованої опортуністичної поведінки політичних акторів, спрямованої на реалізацію владних інтересів і набуття певної користі від участі у політичному процесі;

– комплексом неформальних норм, які структурують, обумовлюють дії політичних акторів, суперечать колективним ідеалам, цілям, увиразненим у формальних інститутах;

– закритим від громадськості видом політичних практик у непублічному полі комунікації;

– неформальним інститутом, який зумовлює заміщення формальних інститутів неформальною інституціалізацією;

– систему соціальних правил, зазвичай неписаних, що створені та виконуються за межами офіційно дозволених каналів. Механізм політичної корупції спирається як на правові норми, які уможливлюють зловживання та містять правові прогалини, так і, більшою мірою, на неформальні правила» (Кушнарьов, 2018, с. 90-91). Більш детальний опис видів, форм та моделей політичної корупції подає у своїй монографії Г. Кохан (Кохан, 2013).

Нарешті, остання типізація за рівнем прояву корупції. З юридичного погляду, рівнями корупції можна було б виділити такі, що знаходять свій вияв у 1) корупційних діяннях (усі прояви корупції, які є суспільно небезпечними); 2) корупційних правопорушеннях (частина (вид) корупційних актів, заборонених законом, за які встановлена юридична відповідальність різних видів). Виходячи з цього В. Трепак пропонує розглядати корупцію на таких рівнях як:

1) окреме (корупційне) діяння): корупційний злочин, корупційне правопорушення;

2) корупційна злочинність;

3) комплексне загальнонаціональне суспільно-правове явище, що охоплює усі корупційні (корупціогенні) фактори;

4) міжнародне явище (Трепак, 2020, с. 54).

3. Напрями, моделі, форми і способи попередження корупції.

Від моделей корупції ми плавно переходимо до напрямів, моделей, форм і способів попередження цього феномену. Кожна держава намагається знайти свою стратегію попередження / протидії корупції, яка зумовлена як динамікою корупції, станом економіки та специфікою правової системи і культури суспільства, так і змістом конкретних заходів щодо попередження корупції (Мельник & Хавронюк, 1998). Адже невідповідний розподіл ресурсів та визначення пріоритетних цілей щодо протидії корупційним правопорушенням може призвести до протилежних наслідків.

В контексті будь-якої держави об’єктом попередження має бути корупція як комплексне, загальнонаціональне суспільно-правове явище. Боротьба з

окремими корупційними діяннями або з корупційною злочинністю не дадуть очікуваного результату, оскільки системність даного явища буде компенсувати успіхи, досягнуті лише в окремих сферах (Трепак, 2020, с. 55). Головними суб'єктами попередження корупції в державі є держава в особі органів державної влади та місцевого самоврядування та народ в особі громадян та інститутів громадянського суспільства.

Якщо мова йде про попередження / протидію корупції, треба розмежовувати заходи і засоби, що будуть суттєво відрізнятися у випадках:

1) попередження / протидії вчинення окремих корупційних правопорушень некримінального характеру;

2) попередження / протидії вчинення окремих корупційних злочинів;

3) попередження / протидії організованій (корупційній) злочинності;

4) попередження / протидії корупції як комплексному загальнонаціональному суспільно-правовому явищу;

5) попередження / протидії корупції як галузевому явищу (в політичній, правоохоронній, освітній, медичній сферах та ін.);

6) попередження / протидії корупції на міжнародному рівні.

Оскільки корупція – це системна проблема, то для попередження їй необхідне застосування системного підходу, що полягає в узгодженні дій влади, бізнесу та громадянського суспільства. Як зазначає В. Трепак (Трепак, 2020, с. 250), заходи з попередження / протидії корупції поділяються на дві групи:

1) заходи з посилення боротьби з корупційними проявами;

2) заходи з боротьби із інституційними передумовами, що створюють корупцію – ознаками потенційної корупції, із посадовою особою, яка за певних умов може стати корупціонером.

Є точка зору, згідно з якою оптимальною буде протидія корупції, заснована на трьох складових: методах усвідомлення, методах попередження та методах запобігання. На думку О. Костенко, кращим варіантом попередження / протидії корупції є розробка та впровадження комплексних технологій попередження / протидії корупції в кожній окремій сфері, оскільки корупція може

пристосуватися до особливостей тієї чи іншої сфери суспільного життя, що може звести нанівець будь-які антикорупційні спроби (О. М. Костенко, 2008, с. 141). Тому автор пропонує концепцію протидії корупції, що ґрунтується на формулі «культура плюс репресія», основна ідея якої полягає в тому, що, радикальним засобом протидії корупції є правова та моральна культура громадян і антикорупційне законодавство разом із профільними інституціями (О. М. Костенко, 2016, с. 12).

Слід зазначити, що причини корупції спричинені станом суспільних відносин у конкретному соціумі. А отже, корупція є не винятковою вадою владного апарату, а симптомом, що свідчить про наявність об'єктивних суспільних проблем – чим складніші ці проблеми, тим вищий і рівень корупції. Для їхнього усунення потрібне вжиття низки комплексних заходів, що часто виходять за межі політологічної науки. Остання у цьому випадку може лише констатувати факт виникнення корупції під впливом того чи іншого чинника та звернути увагу на необхідність його усунення.

На думку В. Гаращук найбільш ефективною є попередження / протидія корупції шляхом усунення основних умов, що її породжують:

– низького рівня життя посадових осіб, уповноважених на виконання функцій держави;

– високих ціни на товари та послуги;

– необґрунтованої конфіскаційної податкової політики держави, за якої виробнику легше підкупити посадову особі та приховати прибутки, аніж платити податки тощо (Гаращук, 1997, с. 124).

Додатково пропонуються заходи щодо:

– забезпечення мінімального втручання держави у бізнес і скасування стимулів до корупції;

– зменшення кількості податків, процедури сплати та звітування;

– зменшення втручання держави у господарську діяльність гравців ринку;

– забезпечення ефективного контролю за антиконкурентною поведінкою великих компаній (Валлє, 2015, с. 172-173).

Розглянемо типологію заходів попередження / протидії корупції за версією М. Кікалішвілі. Перший критерій, найбільш розповсюджений, це угруповувати за змістом та метою застосування, згідно з яким антикорупційні заходи поділяються на профілактичні, що мають на меті усунення соціальних передумов та мінімізацію корупційних ризиків; правоохоронні, які зосереджені на виявленні, припиненні та розслідуванні корупційних правопорушень; репресивні, що передбачають застосування санкцій і примусових заходів до осіб, винних у корупційних діях; а також заходи поновлення, спрямовані на відновлення порушених прав і законних інтересів потерпілих від корупційних зловживань (Кікалішвілі, 2021, с. 203).

За масштабом застосування антикорупційні заходи поділяються на загальнодержавні, які охоплюють усю територію країни та ухвалюються центральними органами влади; регіональні, що діють у межах окремих областей, міст чи адміністративних одиниць; локальні, спрямовані на конкретні установи чи підприємства; а також заходи з цільовим призначенням – як колективного характеру, спрямовані на окремі групи осіб, так і індивідуалізовані, які адресуються конкретним особам (Кікалішвілі, 2021, с. 204).

Антикорупційні заходи також класифікують за терміном дії та нагальністю їх застосування: до невідкладних належать ті, що потребують термінового впровадження; короткострокові заходи реалізуються в обмежені часові рамки через нагальність проблеми; довгострокові орієнтовані на перспективу й передбачають стратегічне планування; а постійно діючі заходи мають безперервний характер і включають, зокрема, моніторинг корупційної злочинності чи системну правоохоронну діяльність (Кікалішвілі, 2021, с. 206).

Міжнародний досвід засвідчує ефективність чотирьох ключових підходів до боротьби з корупцією: застосування психологічних і технічних методів, запровадження чіткої регламентації процесів та використання репресивних

заходів, причому їхнє комплексне поєднання дає змогу істотно зменшити рівень корупції (Шаркова, 2020, с. 193).

Водночас поширена точка зору, що фрагментарне обмеження лише окремих сфер впливу або застосування вузького спектра антикорупційних заходів дає переважно тимчасовий результат. Згодом корупційні практики адаптуються до нових умов, змінюючи як структуру, так і канали отримання неправомірної вигоди, переміщуючись у ті сектори, які залишаються поза досяжністю наявних механізмів контролю. У підсумку загальний обсяг корупційних втрат відновлюється до початкового рівня або навіть перевищує його (Тараненко, 2014).

За ознакою методу впливу антикорупційні заходи можна поділити на:

1) ті, що пов’язані з примусом;

2) ті, що стимулюють правомірну поведінку без вдавання до натиску (Кікалішвілі, 2021, с. 206).

При цьому, примусові заходи поділяються на заходи:

– захисту (правові приписи, що мають на меті запобігти корупційній криміналізації суспільних відносин);

– покарання (різноманітні форми відповідальності за корупційні діяння);

– поновлення (приведення суспільних відносин до того вигляду, який мав місце до вчинення корупційного діяння).

За часом здійснення заходів попередження / протидії корупції виокремлюються:

– заходи, що здійснюються до моменту вчинення корупційного діяння (профілактика);

– заходи, що здійснюються після скоєння корупційного правопорушення (Мельник, 2004, с. 235).

За характером вчинюваних антикорупційних заходів виокремлюються:

– спеціальні заходи (спрямовані на подолання корупції);

– багатофункціональні (впливають як на сам феномен корупції, так і на тотожні йому явища (відмивання коштів, шахрайство тощо).

Власну систему заходів попередження / протидії корупції запропонували А. Суббот і Ю. Дем'янчук (Суббот & Дем'янчук, 2017): 1) оптимізація кількості державних службовців; 2) вдосконалення нормативно-правового забезпечення; 3) врегулювання питань необґрунтованого адміністративного розсуду; 4) використання міжнародного досвіду у попередженні / протидії корупційній злочинності; 5) створення інститутів протидії корупції; 6) антикорупційне виховання населення; 7) масштабне реформування державного управління.

На думку Є. Невмержицького антикорупційна діяльність у державі має здійснюватися у двох основних напрямах:

1) боротьба з корупцією як з кримінальним / адміністративним проявом, що полягає у виявленні, розслідуванні, припиненні та притягненні до відповідальності винних осіб;

2) боротьба з соціально-економічним та політичним підґрунтям корупції із використанням комплексу економічних, політичних, профілактичних, культурних, виховних, організаційних та інших заходів (Невмережицький, 2008).

За результатами соціологічного опитування співробітників органів правопорядку, що було здійснено в рамкам дисертаційного дослідження В. Трепак, перспективними напрямами попередження / протидії корупції на сучасному етапі є:

– виявлення вчинених корупційних правопорушень (мереж, схем та груп);

– притягнення винних у вчиненні корупційних правопорушень до відповідальності;

– усунення умов (ускладнення можливостей) вчинення корупційних правопорушень (зокрема, забезпечення антикорупційної якості законодавства, контроль за законністю доходів, перевірка е-декларацій) (Трепак, 2020).

Крім цього, М. Кікалішвілі акцентує увагу на таких профілактичних заходах як:

– журналістські розслідування, які можуть використовуватися органами правоохоронної діяльності у подальшій роботі (Кікалішвілі, 2021, с. 252);

– комплаєнс-політиці як «системі внутрішнього контролю всередині комерційних та некомерційних організацій на предмет дотримання ними вимог законодавства, зокрема антикорупційного» (Кікалішвілі, 2021, с. 253);

– нестандартні методи, наприклад, проведення фундаментальних наукових досліджень корупційного середовища, корупційних схем або активне використання здобутків науково-технічного прогресу – новітніх інформаційних технологій (Кікалішвілі, 2021, с. 372-373).

Якщо вже говорити про нестандартні методи, то розпочали вони свою історію в сфері поєднання таких дисциплін як соціологія і криміналістика – досліджень Е.Х. Сазерленда, Д. Р. Кресі, С. Альбрехта, Р. Холлінгера, Дж. Т. Уелса (Wells, 2017; Лепський, 2022), в рамках яких корупція розуміється як один із видів шахрайства. Шахрайство, за версією ACFE, це «використання службового становища з метою особистого збагачення шляхом навмисного неналежного використання або зловживання ресурсами і активами організації-роботодавця» (*Occupational Fraud 2022: A Report to the Nations*, 2022). Існуючі форми та види шахрайства умовно поділяються на акти незаконного привласнення активів організації, шахрайство з фінансовою звітністю та, відповідно, корупція (Wells, 2018, с. 9). Тому інструменти та відповідні заходи з протидії феномену шахрайства, на нашу думку, можна з певним успіхом використовувати для попередження / протидії корупції.

Сучасні інструменти попередження / протидії шахрайству, в першу чергу, корпоративному, представлені у вигляді багаторівневих програмних комплексів, що передбачають операції з обробки (перетворення і очищення) даних, аналізу даних (аналітики) та візуалізації даних (звітності). Такі програмні рішення використовують найсучасніші технології машинного навчання, штучного інтелекту засновані на накопичених в компаніях даних, а також методах прогнозної аналітики, аналізі «шахрайських мереж і системи звітності та

управління розслідуваннями, які дозволяють оптимізувати роботу служб безпеки» (Хамига, 2020, с. 153).

В англомовному дискурсі для позначення відповідних практик щодо виявлення, попередження та взагалі протидії шахрайству всередині корпоративного середовища використовується термін «forensic», що згідно з словником Collins, використовується для позначення виду робіт з аналізу доказів під час кримінальних або адміністративних проваджень ("Forensic"). Зазвичай даний термін у поєднанні з терміном «science» перекладається як криміналістика. Так от, фахівці-криміналісти, що мають досвід в сфері виявлення фактів корпоративного шахрайства чи корупції можуть на постійній основі надавати зацікавленим особам так звані forensic-послуги, які передбачають:

– «врегулювання розбіжностей між сторонами конфлікту з фінансових і ділових питань;

– виявлення та аналіз прихованих комерційних ризиків; захист інтелектуальної власності;

– корпоративну (ділова) розвідку;

– недопущення фінансового і репутаційного збитку;

– перевірку контрактних зобов'язань і надійності ділових партнерів;

– перевірку повідомлень по «гарячій лінії»;

– позасудову, досудову експертиза, а також сприяння у ході судових розглядів;

– проведення compliance-розслідування;

– протидію в легалізації незаконних доходів;

– розробку процедур, спрямованих на попередження / протидію шахрайству, корупції, виведенню коштів, привласненню активів;

– розслідування шахрайства з використанням інформаційних технологій; управління ризиками, пов'язаними з шахрайством; фінансова експертиза документів; фінансові розслідування» (Долбнєва, 2019, с. 25-26).

Розглянемо заходи з попередження шахрайства / корупції, які виділяють фахівці ACFE (Wells, 2014). Весь перелік заходів з попередження шахрайства / корупції умовно можна розподілити на 4 категорії:

1. Організаційні методи – методи, що передбачаються створення / функціонування спеціалізованих підрозділів щодо попередження / протидії шахрайству: відділу внутрішнього аудиту, незалежного аудиторського комітету, гарячої лінії чи спеціального відділу / команди з попередження / протидії шахрайства.

2. Освітні методи – методи, що передбачають заходи з навчання персоналу організації в сфері попередження / протидії шахрайству, сертифікацію керівного складу в сфері фінансової звітності.

3. Нормативні методи – методи, що визначають регламенти та процедури щодо випадків шахрайської поведінки та протидії їй: кодекси поведінки, політику організації щодо шахрайства та корупції, системи нагород за викриття шахраїв, програми підтримки співробітників, порядок ротації кадрів та обов'язкових відпусток.

4. Технологічні методи – методи безпосереднього впровадження інноваційних аналітико-статистичних технологій попередження / протидії шахрайству / корупції в організації. До цієї категорії відносяться зовнішній аудит фінансової звітності, аналіз керівництва, зовнішній аудит внутрішнього контролю за фінансовою звітністю, проактивний моніторинг / аналіз даних, формальна оцінка ризиків шахрайства, сюрприз-аудит.

Як зазначає Ю. Хамига, для попередження корпоративному шахрайству використовуються такі інструменти, що працюють за умови їх системного застосування:

– compliance-практики;

– проведення щорічного аудиту фінансової звітності;

– whistle blowing system (WBS) як інструмент впровадження політики нетерпимості до будь-якого роду фактів шахрайства в організації;

– in-house інструменти (зовнішній фінансовий контроль (Хамига, 2020, с. 154-155).

Мовою фахівців ACFE, попередження / протидія шахрайству, в тому числі корупції, пов’язана із процедурою виявлення подібних випадків (detecting), адже виявлення відповідних правопорушень означає можливість визначення можливих заходів. Згідно з останнім звітом ACFE (*Occupational Fraud 2022: A Report to the Nations*, 2022, p. 9), найбільш поширеною категорією шахрайства на робочому місці (occupational fraud) є незаконне привласнення активів (asset misappropriation) – 86%, що передбачає крадіжку або неналежне використання ресурсів роботодавця. Однак, ці схеми, як правило, мають найменше середнє значення втрат – 100 000 доларів США за випадок. На відміну від цього, схеми шахрайства з фінансовими звітами (financial statement fraud), в яких злочинець навмисно спотворює фінансову звітність організації, є найменш поширеними (9%), але найдорожчою категорією – середнє значення втрат за випадок складає 593 000 доларів США. Третя категорія, корупція, до якої включено такі злочини, як хабарництво, конфлікти інтересів і здирництво, – займають середнє місце як за частотою, так і обсягом збитків. Ці схеми трапляються в 50% випадків і спричиняють в середньому втрати у суму в 150 000 доларів США за випадок. При цьому, шахраї не обов'язково обмежують себе однією категорією правопорушення.

З випадків, що були досліджені у звіті, 40% здійснили більше однієї з трьох основних категорій шахрайства. 32% шахраїв вчинили як незаконні привласнення активів, так і корупційні схеми в рамках свого злочину, 2% незаконно привласнених активів скоєно разом із фальсифікацією фінансових звітів, 1% займалися як корупцією, так і шахрайством у фінансовій звітності, а 5% змогли включити всі три категорії до своїх схем (*Occupational Fraud 2022: A Report to the Nations*, 2022, p. 11).

Результати дослідження показали, що деякі засоби виявлення шахрайств / корупції більш ефективні, ніж інші.

Рисунок 2.2.1 – Засоби виявлення шахрайства на робочому місці (*Occupational Fraud 2022: A Report to the Nations*, 2022)

На першому місці за методом виявлення знаходиться «підказка / натяк» (“tip”) – 42%, іншими словами, це значить, повідомлення про випадок корупції. На другому місці (16%) знаходиться метод «внутрішній аудит» (“internal audit”). На третьому «аналіз керівництва» (“management review”) 12%. Взагалі загальний відсоток засобів, в яких можливе застосування аналітико-статистичних технологій складає 50%, тобто: внутрішній / зовнішній аудит (“internal / external audit”), звірка рахунків (“account reconciliation”), експертиза документів (“document examination”), автоматизований моніторинг транзакцій / даних (“automated transaction / data monitoring”), аналіз керівництва (“management review”) та безпосереднє спостереження (“surveillance / monitoring”).

Як зазначають автори звіту, кількість випадків шахрайства, які було кваліфіковано як корупція, за останні 10 років збільшилася з 33% до 50%, про що додатково свідчить статистика змов: кількість шахрайств, здійснених однією особою, зменшилася з 58% у 2012 році до 42% у 2022 році; та збільшилася з 42% у 2012 році до 58% у 2022 році для випадків, здійснених двома і більше особами (*Occupational Fraud 2022: A Report to the Nations*, 2022, p. 19). Також у звіті зазначається про зростання використання шахраями технологій блокчейну разом

з більшою кількістю організацій, що включають використання криптовалюти в свої регулярні операції, що створює ще одну можливість для окремих осіб для провадження шахрайських / корупційних схем. Серед випадків найбільш поширеними способами використання криптовалюти були отримання хабаря і «відкати» (48%) (*Occupational Fraud 2022: A Report to the Nations*, 2022, p. 20).

Закінчуючи підрозділ, можемо констатувати, що держава є складним і багатовимірним простором, у якому відбувається перетин інтересів громадян, еліт і зовнішніх акторів. В ідеальній моделі вона виступає гарантом справедливості, рівності та публічного блага. Однак реальні процеси функціонування держави нерідко демонструють її трансформацію у простір, де приватні інтереси заміщують суспільний інтерес, а механізми влади використовуються для збереження або посилення привілеїв окремих груп.

Концепція держави як корпорації дозволяє пояснити, як інституційні механізми делегування повноважень і прийняття рішень можуть стати джерелом корупційних ризиків у разі викривлення принципів підзвітності й прозорості. Політична система, у межах якої функціонує держава, відіграє визначальну роль у формуванні або стримуванні простору корупції. У нерозвинених або деформованих політичних системах корупція еволюціонує у структурне явище через захоплення інституцій держави економічними чи політичними елітами.

Якість урядування є критичним фактором, що визначає здатність держави бути простором спільного життя, а не ареною приватизації ресурсів. Високий рівень неупередженості, компетентності й підзвітності інституцій є основною умовою стримування корупційних практик. Натомість слабке врядування сприяє переходу корупції з окремих випадків у системну норму.

Міжнародні антикорупційні ініціативи мають потенціал підтримувати інституційну якість держав, однак їхня ефективність прямо залежить від наявності внутрішньої політичної волі до змін. Зовнішній тиск без реального перерозподілу влади і реформування стимулів часто лише стабілізує існуючі патерни корупції.

Інституційні деформації – такі як розмиття меж між приватним і публічним, фаворитизм, зрощення державного і корпоративного сектору – є головною причиною перетворення держави з організатора спільного життя у простір відтворення структурної корупції.

Отже, держава має подвійний характер: вона залишається водночас і необхідним інструментом організації суспільства, і потенційним механізмом зловживання владою. Успішне попередження / протидія корупції вимагає не тільки технічних заходів, але й глибинного інституційного переосмислення самої природи влади і її організації у суспільстві.

Корупція у межах державного простору проявляється як складне багаторівневе явище, яке охоплює всі сфери суспільного життя – від побутових взаємодій до формування політики на найвищих щаблях влади. Моделі та форми корупційних практик варіюються залежно від характеру політичного режиму, рівня економічного розвитку, якості інституцій та загальної культури суспільства. Корупція може набувати системного характеру через викривлення державних функцій, коли інститути влади, замість служіння суспільному благу, починають обслуговувати приватні інтереси окремих еліт чи корпоративних груп.

Різноманітні типології корупції, що охоплюють політичну, адміністративну, соціальну та економічну сфери, демонструють багатогранність цього явища і необхідність застосування диференційованих стратегій попередження / протидії. Системна природа корупції вимагає одночасного впливу як на окремі правопорушення, так і на глибинні причини її виникнення – політичні, соціальні та економічні умови, що породжують сприятливе середовище для корупційних практик.

Моделі боротьби з корупцією, сформовані в міжнародній і національній практиці, виявляють як ефективні, так і обмежені інструменти впливу. Водночас результати досліджень підкреслюють: без комплексного підходу, що поєднує репресивні, профілактичні, організаційні та освітні заходи, подолати корупцію неможливо. Особливого значення набуває розмежування заходів за рівнями і

сферами застосування – від загальнонаціональних стратегій до галузевих і локальних програм втручання.

Важливим компонентом сучасної антикорупційної політики є інтеграція інноваційних аналітико-статистичних технологій, які дозволяють не лише виявляти вже вчинені корупційні правопорушення, але й будувати превентивні системи раннього попередження ризиків. Використання інструментів судово-бухгалтерської експертизи (forensics), цифрового моніторингу, інтелектуального аналізу даних (data mining), блокчейн-технологій та краудсорсингових платформ радикально розширює можливості для прозорості, підзвітності й контролю над діями посадових осіб.

Таким чином, ефективне попередження / протидія корупції потребує комплексного розуміння її багаторівневої природи, системної інтеграції класичних і інноваційних підходів, а також активної участі усіх акторів суспільного життя – державних органів, бізнесу, громадянського суспільства і міжнародних партнерів. Успішність антикорупційної стратегії визначатиметься не тільки кількістю викритих правопорушень, а насамперед глибиною трансформації інституційних і культурних передумов, що породжують і відтворюють корупційні ризики.

2.2. Зміст та класифікація аналітико-статистичних технологій

1. Цифрова трансформація держави.

Одним з пріоритетних напрямків розвитку України на сучасному етапі розвитку, не враховуючи російсько-українську війну, є цифрова економіка, «держава в смартфоні» або концепція держави як інформаційної платформи (Кивлюк, Гарбар, Пунченко, Арабаджиєв, & Андрюкайтене, 2024). Головною ідею цієї концепції є досягнення благополуччя громадян та полегшення економічного зростання на основі впровадження інноваційних інформаційних технологій ("Про нас," 2023). В центрі цієї платформи знаходиться громадянин у цифровій реальності. Держава в цьому питанні має створити такі умови, що допоможуть окремій людині відкрити свої можливості, сформувати комфортне і

безпечне середовище для повсякденного буття громадян за рахунок впровадження всіх інноваційних технологій, які до цього в більшості випадків використовувались з бізнес метою. Серед позитивних наслідків цифровізації держави вважається зменшення адміністративних витрат та навантаження щодо надання різного роду звітності за рахунок створення додаткових каналів комунікації між громадянином і державою (Kryvoshein, 2023). При цьому бізнес отримає можливість взяти безпосередню участь у розробці та підтримці цієї системи. В свою чергу, громадяни отримають можливість отримувати всі послуги, як від держави, так і частково від бізнесу, у цифровому вигляді – новою якістю, за більш коротші терміни, з більшою швидкістю. Найголовніше, саме цифровий формат надання / отримання послуг мінімізує контакт із представниками влади, що є одним із чинників мінімізації корупції, точніше, дрібної корупції.

Найбільш перспективними інформаційними технологіями з точки зору їх активного застосування у будь-якій дослідницькій (в тому числі аналітико-статистичній) діяльності (*Applied Informatics for Industry 4.0*, 2023; Lepskyi, Kudinov, Lepska, & Rusetsky, 2023; Rudnieva, 2024) є:

– технології збереження даних, в тому числі хмарні технології (cloud computing) та технології великих даних (big data analytics);

– технології штучного інтелекту (artificial intelligence) та пов’язані із ними технології відтворення людського мислення та розуму (нейротехнології);

– технології захисту даних та системи розподіленого реєстру (blockchain);

– виробничі (промислові) технології, пов’язані із забезпечення матеріально-технічної бази інформаційних технологій (нанотехнології, технології комунікації та зв’язку);

– робототехніка і сенсорні технології;

– технології віртуальної та доповненої реальності.

Першочерговою технологією в цьому напрямі є технологія великих даних (Big Data), що включає можливості зберігання даних у різному форматі та формі

структурованих / не структурованих / напівструктурованих баз даних, в тому числі, реляційних баз даних, включаючи табличні форми подання цих даних та документальні бази даних у формі цифрових документів (зображень, аудіо, відео) (D. Li & Xu, 2022). Ці дані фіксують факти економічної активності певних окремих організацій, секторів національної економіки та представляють інтерес з точки зору отримання корисних висновків заснованих на них.

Наступна технологія, що побудована на великих даних, це технологія штучного інтелекту як можливість виключити людину з процесу прийняття рішень, залучення машин до процесу адаптації масивів даних до реальних життєвих ситуацій (Kejriwal, 2023).

Розподілені системи реєстру або так звана технологія blockchain – це технології побудови обміну транзакціями і доступу до інформації, що забезпечують необхідний рівень інформаційної безпеки (зменшення ризику крадіжки, шахрайства, порушень майнових прав) та забезпечення прозорості, відкритості, децентралізації інформаційних систем (*The Data-Driven Blockchain Ecosystem: Fundamentals, Applications, and Emerging Technologies*, 2023). Не можна обговорювати жодних технологій без якісно організованих каналів комунікацій, тому промислові Інтернет-технології є ключовими для побудови цієї інформаційної та комунікаційної інфраструктури.

Якщо ми говоримо про можливості використання цих технологій як інструментів автоматизації розумової діяльності або так звану «цифрову трансформацію» – виникає питання, чому саме трансформація? Річ у тому, що всі ці технології дозволяють перетворювати усталені форми господарювання, ведення бізнесу, взаємодії між громадянами, суспільством та бізнесом та нарешті мислення. Ключовою тут є ідея використання даних у процесі управління. Вона не нова, однак лише саме поява технології big data дозволила управління на основі даних звести до рангу інформаційної культури. Саме зараз професії бізнес-аналітик (business analyst), системний аналітик (systemic analyst), аналітик даних (data scientist) та інші фахівці з аналізу даних, машинного навчання

користуються попитом не лише в комерційному секторі, але й у державному (Awati & Scriven, 2023).

Процес використання даних від самих даних до рішення, як на оперативному, тактичному, так і на стратегічному рівні, передбачає використання не лише засобів переробки даних в інформацію (звіти) чи інструментів аналізу, але й також інструменти моделювання (опису певних процесів мовою математики) та створення прогностичних моделей, які дозволяють приймати рішення з орієнтацією на майбутнє. Для цього необхідні не просто дані, а правильно відібрані дані, технології їх обробки, технології їх візуалізації та, звичайно, моделювання.

Процес цифрової трансформації передбачає трансформацію щонайменше трьох суб'єктів соціальної взаємодії – громадянина, держави та бізнесу, за результатами якого громадяни мають отримати високоякісний цифровий продукт, в межах якого і будуть розвиваються їх подальші відносини. Головним тут є не лише орієнтація на дані, але й сервісно- та процесно-орієнтований підхід, що передбачає інтеграцію та підтримку людини на всіх етапах життєдіяльності, пов'язаних із отриманням будь-то державних чи комерційних послуг на основі однієї цифрової платформи.

Як результат, необхідно якось створити та розробити цю цифрову платформу на основі існуючих технологій, тобто аналітико-статистичних технологій, технологій розподіленого реєстру, збереження даних, штучного інтелекту тощо. Для кожної цієї технології мають бути розроблені сервіси, засновані на даних. Крім цього, не слід забувати про те, що деякі з інноваційних технологій є службовими (штучний інтелект, Інтернет речей, технології доступу та ідентифікації), тобто за допомогою використання цих технологій покращується процес цієї взаємодії. В свою чергу, сервісний та процесний підходи дозволяють не тільки організовувати цей процес, але й по-різному будувати відповідні бізнес-процеси, а значить по іншому відбудовувати логіку взаємодії учасників інформаційного простору.

Слід зауважити, що всі ці підходи породжені комерційною сферою, що поступово починає розповсюджуватися на дотичні їй сфери. Орієнтація на клієнта призвела до зміни у підході щодо формування виробничого процесу, а саме до мінімізації витрат або зменшення кількості посередників між клієнтом та виробником того чи іншого цифрової / нецифрового продукту. Для цього необхідно не лише з'єднати їх через сервіс-орієнтовану архітектуру інформаційної системи, але й потрібно буде запровадити державу, орієнтовану на послуги. У той же час, держава, звичайно, має взяти на себе роль координатора та управління взаємодією всіх учасників платформи. Тобто ця платформа повинна бути єдиною та базовою, яка може інтегрувати в себе і бізнес-рішення, наприклад, банківський сектор. Тому для забезпечення якості цієї платформи, відповідності її попиту громадян необхідна підтримка постійного та зворотного зв'язку, тобто клієнтоорієнтований підхід (Кіндратець, 2022).

Для цього необхідно використовувати надійні та єдині дані для прийняття рішень, тому цифрова платформа має містити єдину базу даних, в якій кожен суб’єкт, будь-то окремий орган державної влади, окрема організація чи окремий громадянин повинні бути ідентифіковані. Саме для цього існує галузь технологій підтвердження доступу, включаючи технології кваліфікованих електронних підписів, біометричні технології тощо.

В основі цифрової держави має бути людина із цифровим менталітетом – тобто людиною, що приймає цифрову реальність такою, яка вона є, і здатна ефективно працювати в ній. І як ми бачимо зараз, це скачкоподібний процес. Спочатку він розвинувся у бізнесі, а ось тепер дійшов до органів державної влади. Адже зараз багато людей розуміють, що уникнути від подальших трансформацій неможливо.

Якщо ми говоримо про можливості трансформації, то ця трансформація може відбуватися по-різному. Історично вдосконалення цифрової платформи, яка зараз розвивається і починає будувати нашу країну, може пройти у двох напрямках. Перший напрямок (brownfield) – це сценарій для покращення

розвитку мереж відомчих систем (Tureckova, 2021). Не секрет, що з початку 2000 року в нашій країні розроблялися різні розрізнені відомчі платформи та відомчі інформаційні системи, що дозволило отримувати цифрові послуги, включаючи електронні форми, головним чином, звичайно, не в проактивних і не в життєвих ситуаціях, а лише в одному із напрямків. Ця еволюція державної системи передбачала збереження цих відомчих систем та вдосконалення обміну інформацією між ними. Україна спочатку обрала цей напрямок.

Розуміння необхідності обрати другий шлях (greenfield) (Bayar, 2017) відбулося лише після того, як ця можливість справді виникла – з 2018 року ("Цифрові трансформації в Україні: чи відповідають вітчизняні інституційні умови зовнішнім викликам та європейському порядку денному?," 2020). У 2018 році уряд затвердив Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки. Починаючи з 2019 року в Україні було створено відповідне відомство (Міністерство цифрової трансформації), що почало реалізовувати низку заходів щодо переведення української економіки в цифровий формат ("Наполеоновские планы | Цифровая ЗеУкраина: план развития digital-экономики," 2019). На першому етапі було здійснено оформлення нормативної бази та збільшення доступності технологій разом із зниженням вартості програмного забезпечення, комп’ютерного та іншого обладнання. Передумовами просування цифрового порядку денного України належать розроблене законодавство про цифрову економіку та телекомунікації, цифрову інфраструктуру, в тому числі, розвиток електронної торгівлі, електронного захисту та кібербезпеки ("Про хмарні послуги. Закон України від 17.02.2022 №2075-IX," 2022).

У той же час виникла проблема нових цифрових бізнес-процесів на основі даних. Було вирішено відмовитися від багатьох існуючих розробок і побудувати нову екосистему на основі архітектури обслуговування, яка передбачала радикальну зміну підходів до організації процесів за моделлю провідних IT-компаній – так з’явився проект «Держава і Я» або ДІЯ. Завдяки цьому продукту Україна змогла стати першою «цифровою» державою у світі. Цифровою в тому

сенсі, що поступово кожний з напрямків надання державних послуг проходить етапи реорганізації, реінжирінгу всіх управлінських процесів із широким використанням цифрових інструментів. Під цифровими інструментами розуміються механізми виконання процесів, що призводять до появи нових властивостей цифрових продуктів та прийняття рішень в автоматичному режимі без участі людини. На нашу думку, цифрова трансформація держави – це не лише трансформація управлінських процесів, але й трансформацію людини та породженій нею культури споживання цифрових продуктів, культури взаємодії із інформаційними системами, яким ми приділемо нашу подальшу увагу.

2. Сутність інформаційних технологій.

Щоб зрозуміти їх зміст, нам доведеться розібратися із сутністю більш загального феномену під назвою «інформаційні / цифрові технології». Інформаційні технології (informational technologies) можуть бути представлені як поєднання трьох основних методів перетворення інформації: зберігання, обробки та передачі (Pintar & Hopping, 2023). Вся історія їх формування нерозривно пов’язана з формуванням та розробкою цих трьох методів, згрупованих за чотири періоди.

Перший етап розвитку пов’язаний із використанням найбільш примітивних форм передачі сигналу – звукових коливань (танці, пісні, усні традиції). Другий етап розвитку пов’язаний з активним використанням штучних носіїв інформації та технологій нанесення зображень та символів на матеріальні носії (печерний живопис, гравірування кісток). Третій етап розвитку пов’язаний із появою писемності, що дозволило збільшити кількість накопичення даних на матеріальних носіях і, в свою чергу, якість та тривалість зберігання даних. У той же час, діапазон матеріалів, що використовуються в якості носіїв інформації. Саме в цей період відбувається перша ІТ-революція – винахід друку, що дозволило розширити коло прямих користувачів інформаційних ресурсів – священики втратили ексклюзивне право на доступ до джерел знань. Друга ІТ-революція (створення комп’ютерів) була початком четвертого етапу розвитку ІТ, під час якого також відбувається третя ІТ-революція – створення інформаційно-

обчислювальних (комп'ютерних) мереж, що дозволили поєднати одиничні обчислювальні потужності у так звані кластери та навіть, в певному сенсі, єдине інформаційно-обчислювальне середовище, яке деякі дослідники порівнюють з нейронною мережею та обговорюють питання появи та розвитку нейронної мережі планети і формування планетарного розуму (Крохмаль, 2004).

Починаючи з цьому часу науковці говорять про так званий інформаційний етап розвитку суспільства, проявом якого вважається перехід людства до планетарного рівня розвитку (Шаховська, 2022), збільшення темпів подвоєння інформації (Wiener, 1954) та перевищення витрат кожної окремої держави на розвиток інформаційних технологій порівняно з витратами на енергетику (Martin, 1977). У епоху інформації відбувається так звана інформатизація суспільства, що виявляється в активному впровадженні комп'ютерів та відповідних засобів комунікації в існуючі сфери людської діяльності.

Головна роль на цьому етапі розвитку суспільства належить галузі виробництва технічних засобів, методів та технологій для виробництва нового знання, що забезпечує безкоштовний доступ до будь-яких джерел інформації, за винятком законодавчо засекречених.

Відповідно, серед усіх існуючих типів людської діяльності виділяється той його тип, що забезпечує пошук, збір, створення, обробку, організацію, зберігання, розповсюдження та використання інформації – інформаційна діяльність. У структурі інформаційної діяльності вирізняються дві відносно незалежні сфери: 1) інформаційне виробництво та 2) інформаційне самообслуговування (Eischen, 2002). Розподіл на ці сфери пояснюється характером завдань, що вирішуються, та кваліфікацією суб'єкта інформаційної діяльності.

Слід розуміти, що обсяг інформаційного самообслуговування є вторинним стосовно галузі виробництва інформації, метою якої є формування (створення, обробка, організація, розподіл) інформаційного ресурсу суспільства та організація доступу до нього. Саме в цій галузі звично виділити поняття «інформаційні технології», значення якого спочатку було пов'язано виключно з

розробкою комп’ютерних технологій, автоматизованими інформаційними системами, програмним забезпеченням та технічною підтримкою.

На сучасному етапі розвитку інформаційні технології визначаються, у вузькому значенні, як спосіб виробництва інформаційних продуктів та послуг необхідної якості та кількості з оптимальними витратами з урахуванням поточних умов та часових витрат; та в широкому значенні – як набір раціональних методів та засобів інформаційної діяльності, що забезпечують запланований результат (Бутенко & Сирий, 2020).

Як і в будь-якій іншій галузі виробництва, виробництво інформації ґрунтується на функціонуванні реальних підприємств, установ, організацій, предметом діяльності яких є інформація, а кінцевим продуктом є інформаційні продукти та послуги. Їх поєднання породило окрему галузь економіки – інформаційну галузь, що має безпосереднє відношення до створення, обробки, організації та розповсюдження всіх типів інформації, виробництва необхідного програмного забезпечення та обладнання для цього.

Сучасні інформаційні технології суттєво не відрізняються від промислових, однак мають свою специфіку, що проявляється в переважанні інтелектуальної праці, різноманітності асортиментів продуктів та послуг, невеликих, порівняно з промисловістю, обсягах товарів та послуг одного найменування. Основна різниця між інформаційними технологіями та технологіями матеріального виробництва полягає в тому, що: по-перше, інформаційна технологія не може бути безперервною, оскільки вона поєднує в собі роботу рутинного типу (аналіз, облік, контроль) та творчої роботи, яку важче формалізувати (прийняття управлінських рішень); по-друге, процес матеріального виробництва є безперервним і таким, що відображає сувору послідовність усіх операцій для виробництва (технологічний виробничий процес).

Можна виділити два напрямки застосування комп’ютерних технологій у задачах управління якістю, в тому числі якістю роботи політичних інститутів, процесів та ситуацій і самої держави. Перший напрямок пов'язаний із

використанням універсальних чи спеціальних програмних продуктів для статистичних розрахунків під час вирішення конкретних виробничих завдань. Другий напрямок полягає у створенні комп'ютерної системи управління якістю на основі CALS-технологій, до складу якої входить база даних про застосовувані статистичні методи, включаючи системи збору, реєстрації, зберігання та обробки даних про якість.

1. Серед універсальних програмних засобів, встановлених практично на кожному комп'ютері, найбільш поширені електронні таблиці Microsoft Office Excel, які надають досить широкі можливості для статистичного аналізу з використанням статистичних функцій, інструменту для побудови лінії тренду, вбудованого пакета аналізу даних. Набагато ширший спектр інструментів мають статистичні пакети SPSS, SAS, STATA, Statistica та ін.

2. CALS-технології – це підхід до проектування та виробництва, що полягає у використанні комп'ютерної техніки та сучасних інформаційних технологій на всіх стадіях життєвого циклу виробу (Petruf, Madarász, & Kolesár, 2011). Інформаційна підтримка реалізується відповідно до вимог системи міжнародних стандартів, які регламентують правила зазначеної взаємодії переважно за допомогою електронного обміну даними. CALS-технології дають змогу набагато зменшити обсяг проектних робіт. Зумовлено це тим, що більшість вузлів систем, машин і устаткування здійснюється у спеціальних уніфікованих форматах інформації мережевих серверів. Це такий особливий засіб, за допомогою якого відбувається інтеграція промислових автоматизованих систем керування підприємством (АСК) до однієї загальної багатофункціональної системи. Найпростіший приклад таких систем – це будь-які ERP системи на кшталт Salesforce, BAS та їх аналогів.

Аналітико-статистичні технології є однією з форм інформаційних технологій, тому вони мають всі вищезазначені характеристики родового поняття, а отже, має подібні особливості з інформаційним виробництвом. Мета аналітико-статистичної технології – ефективне виробництво інформаційних продуктів та раціональне використання інформаційних ресурсів у процесі

задоволення інформаційних потреб користувача. Об’єкти аналітико-статистичної технології – це інформація (в основному документальна) та запити споживачів. Номенклатура та зміст процесів аналітико-статистичної технології сучасною наукою та практикою однозначно не визначені. Однак у нормативно-правових актах що стосуються питань інформатизації, науковій та навчальній літературі до інформаційних найчастіше відносять процеси збору, обробки, накопичення (зберігання, організації), пошуку та розподілу інформації.

Результатом функціонування аналітико-статистичної технології може бути інформація та/або послуга, які різні за вмістом та формою. Будь-яка аналітико-статистична технологія в її практичному застосуванні (на рівні організації, регіону, галузі, держави, світу) існує у формі (або породжує) інформаційну систему. Інформаційна система – це організаційно впорядкований набір документів (масиви документів) та інформаційних технологій, включаючи використання комп’ютерних та комунікаційних фондів, що впроваджують інформаційні процеси. Інформаційні системи мають надзвичайно широкий спектр застосування в галузі науки, економіки, культури, політики, мистецтва та приватного життя.

3. Класифікація інформаційних технологій.

Різноманітність інформаційних технологій та сфери їх практичного застосування породжують необхідність розвитку теоретичних та емпіричних класифікацій. Як підстави для емпіричної класифікації інформаційних технологій, експерти використовують різні критерії: сфера, тип інформації та методу її обробки, характер інформаційних процесів та метод їх впровадження, тип інформаційного носія, контингент та рівень навчання користувачів, ступінь об’єднання технологічних рішень, рівень інтеграції тощо. В рамках нашого дослідження ми розглянемо лише ті варіанти класифікацій, під які тим або іншим чином підпадають аналітико-статистичні технології.

За критерієм сфери застосування розрізняють (Pintar & Hopping, 2023; Бутенко & Сирий, 2020):

1. Базові інформаційні технології не призначені для прямого впровадження конкретних інформаційних процесів, але є лише тими основними компонентами, на базі яких розробляються прикладні інформаційні технології. До подібних технологій відносять:

– технології баз даних – технології для проектування, обслуговування та експлуатації баз даних різного вмісту та цілей;

– гіпертекстові технології – технології нелінійної організації текстової інформації у вигляді багатьох фрагментів тексту (тез, інформаційних одиниць, вузлів) з чітко зазначеними асоціативними відносинами (зв'язками) між ними;

– мультимедійні технології – технології, що дозволяють створювати, зберігати і використовувати різні види інформації (текст, звук, графіка, фотографії, відео, анімація, запахи) в однорідному цифровому представленні;

– технології програмування – технології розробки, експлуатації та обслуговування комп'ютерних програм;

– телекомунікаційні технології – технології віддаленої комунікації, передача аудіо- та відео-інформації на відстань за допомогою технічних засобів (телеграф, телефон, факс, радіо, телебачення, комп'ютер тощо);

– геоінформаційні технології – технології, які забезпечують роботу з даними про просторово розподілені об'єкти, процеси, явища та події;

– технології штучного інтелекту – технології розвитку та експлуатації інформаційних систем, які можуть накопичувати, класифікувати та оцінювати знання про світ; поповнювати та узагальнювати знання за допомогою логічного висновку; спілкуватися з людиною мовою, близькою до природньої, допомагати їй за рахунок знань, що зберігаються в пам'яті, та логічних засобів міркувань;

– технології захисту інформації – технології захисту інформаційних продуктів (інформаційний масивів, документів, програм, баз та банків даних, тощо) від несанкціонованого використання, спотворення або руйнування.

2. Прикладні інформаційні технології – технології, які реалізують типові методи роботи з інформацією, адаптованими до конкретних областей застосування, наприклад, в: управлінні, промисловому виробництві, торгівлі,

освіті, медицині тощо. У цих сферах застосування інформаційних технологій інформація (дані, інформаційні повідомлення, інформаційні продукти) виступають як ресурс, засоби, правила або проміжний продукт, але не є його кінцевим продуктом. Основним завданням прикладних інформаційних технологій є забезпечення раціональної організації інформаційних процесів, що здійснюється шляхом адаптації до конкретного використання однієї або декількох основних інформаційних технологій, які дозволяють найкраще впроваджувати індивідуальні фрагменти цього процесу.

3. Спеціальні (предметні) інформаційні технології – технології що є специфічними для конкретних напрямків виробництва інформації, наприклад: архівні технології, видавничі технології, рекламні технології, офісні технології, захисні та аналітичні (в тому числі статистичні) технології тощо. У цих технологіях інформація діє не лише як предмет праці та її проміжних результатів, але й як кінцевий продукт діяльності. Названі галузі спеціалізуються на задоволенні потреб суспільства в інформації (виробництво інформаційних продуктів та надання інформаційних послуг).

Отже, відповідно до даної типології інформаційних технологій, аналітико-статистичні технології як завершена (функціонуюча) інформаційна система відноситься до спеціальних інформаційних технологій.

Наступний критерій класифікації – це призначення інформаційної технології (Pintar & Hopping, 2023; Бутенко & Сирий, 2020):

1. Інформаційні технології підтримки (забезпечення) – це технології обробки інформації для вирішення спеціалізованих питань: обробки тексту, роботи з базами даних, мультимедійні технології, розпізнавання, телекомунікації, захисту інформації, розробки програмного забезпечення тощо.

2. Функціональні інформаційні технології – це технології, що реалізують стандартні процедури обробки інформації: технології роботи з офісною документацією, технології роботи з фінансовою інформацією, освітні інформаційні технології тощо, корпоративні інформаційні технології, автоматизовані технології проектування тощо.

В даній типології аналітико-статистичні технології мають безпосереднє відношення до функціональних інформаційних технологій, оскільки інформаційні системи, що створюються цим типом технологій завжди передбачає досягнення мети, що визначається керівним апаратом організації, підприємства, місцевої, регіональної, національної і тому подібної влади.

Відповідно до ступеня охоплення завдань управління виділяють такі типи інформаційних технологій (Pintar & Hopping, 2023; Бутенко & Сирий, 2020):

1. Інформаційні технології обробки даних – технології автоматизації рутинних (повторюваних) операцій управлінської діяльності з метою підвищення продуктивності персоналу. Характерною особливістю цього класу технологій є їх побудова без перегляду методології та організації процесів управління.

2. Інформаційні технології автоматизації офісної діяльності – спрямовані на організацію та підтримку комунікаційних процесів як в організації, так і із зовнішнім середовищем. В них реалізуються типові процедури з діловодства та контроля управління:

– обробка вхідної та вихідної інформації;

– збір та подальше створення звітності протягом певних періодів часу відповідно до різних критеріїв відбору;

– зберігання отриманої інформації та забезпечення швидкого доступу до інформації та пошуку необхідних даних.

Ці технології передбачають наявність інтегрованих пакетів прикладних програм: текстового та/або табличного процесору, електронної пошти, застосунків для аудіо-, відео зв’язку/конференцій, спеціалізовані програми для впровадження електронного управління документами тощо.

3. Інформаційні технологій управління. Мета цього типу інформаційних технологій – задовольнити інформаційні потреби працівників, які приймають рішення. Ці технології орієнтовані на всебічне рішення функціональних проблем, формуванні регулярної звітності та роботи в інформаційно-довідковому режимі для підготовки управлінських рішень.

4. Інформаційні технології прийняття рішень – технології для аналітичної роботи та формування прогнозів, підготовки бізнес-планів та аналітичних висновків щодо досліджуваних процесів та явищ виробничо-господарської практики. Характеристики цих технологій зосереджуються на вирішенні важко формалізованих проблем, генерування можливих рішень, їх оцінки, вибору та наданні користувачеві найкращого з них та аналіз наслідків обраного варіанту рішення.

5. Інформаційні технології експертних систем – це інструменти автоматизації аналітичної діяльності. На відміну від попереднього типу технологій, тут основою для створення продукту / послуги стає накопичений та збережений досвід оцінювання ситуацій, тобто відомостей, що складають базу знань у певній тематиці. Така інформація, що оброблена відповідно до певних правил, дозволяє підготувати розумні рішення та розробити стратегії управління та розвитку.

Аналітико-статистичні технології згідно даної класифікації можуть бути віднесеними щонайменше до трьох типів: управління, прийняття рішень та експертних систем, оскільки кожний з цих типів має безпосереднє відношення до процесу прийняття рішень, що може відбуватися автоматизовано (управління), напівавтоматизовано (прийняття рішень) та у ручному режимі (експертна система). В той же час, функціонування вказаних технологій неможливе без застосування технологій обробки даних та офісних технологій, оскільки вони відповідають за формування баз даних, без яких функціонування аналітичних чи статистичних алгоритмів неможливе.

4. Аналітико-статистичні технології.

Вважаємо за потрібне поринути в сферу тих інформаційних технологій, що визначають атрибутивні властивості будь-яких аналітико-статистичних технологій, оскільки саме завдяки цим технологіям породжуються інтелектуальні (≈аналітичні) інформаційні системи інформаційно-пошукового, експертного, розрахунково-логічного, діагностичного, моніторингового, навчального, проектного характеру.

Ядром такої інтелектуальної системи є база знань – набір фактів, що описують тематичну область, та правила їх логічної (автоматизованої) обробки, що дозволяє робити висновки, які відсутні в базі знань в явному вигляді. База знань включає в себе такі підсистеми як: база фактів (даних), база правил, база процедур (прикладних програм), база закономірностей, база метазнань (знання про саму систему), база цілей (сценарії обробки інформації) та система управління базами знань.

Найпоширенішим класом інтелектуальних систем є експертні системи, які відтворюють діяльність експерта (консультанта) у певній тематичній області знань, тобто імітують саму людину. Саме для цього були створені вже згадані нами технології штучного інтелекту та машинного навчання.

У вузькому значенні, штучний інтелект – це одна з областей інформатики, метою яких є розробка апаратних та програмних засобів, які дозволяють звичайному користувачеві, що не має досвіду програмування, визначати та вирішувати свої завдання, що традиційно вважаються інтелектуальними завданнями, спілкуючись з комп’ютером на обмежених підмножинах природньої мови (I. Gupta & Nagpal, 2020; P. Gupta & Bagchi, 2024). Машинне навчання можна визначити як набір методів, за допомогою яких комп’ютери розпізнають шаблони в даних і використовують ці шаблони для прогнозування (Lantz, 2023).

Реалізація даних методів можлива у вигляді комп’ютерних програм (моделей), які можуть отримувати доступ до даних і вивчати їх. Штучний інтелект використовує комп’ютери для автоматизованого прийняття рішень або розробки рекомендацій. Автоматизовані рішення можуть бути безпосередньо реалізовані або запропоновані людині, яка приймає рішення. Штучний інтелект можна розглядати як «розумну автоматизацію», а машинне навчання – як створені комп’ютером «прогнози на основі даних». Машинне навчання є складовою штучного інтелекту та дає змогу прогнозувати на основі даних. Таким чином, машинне навчання може застосовуватися для підтримки процесу прийняття рішень, але не є обов’язковим чи важливим компонентом (Cassell, 2021).

Серед багатьох продуктів штучного інтелекту є кілька провідних напрямків або когнітивних технологій (*Megatrends 2020 and beyond*, 2020), які зараз викликають найбільший інтерес серед дослідників та практиків (I. Gupta & Nagpal, 2020, p. 5-6): представлення знань та розвитку систем на основі знань (knowledge-based systems); програмне забезпечення систем штучного інтелекту (software engineering for AI); розробка природних лінгвістичних інтерфейсів та машинного перекладу (natural language processing); робототехніка (robotics); машинне начання (machine learning); системи аналізу даних (data mining) та пошуку закономірностей в базах даних (knowledge discovery); розпізнавання шаблонів; нові архітектури комп'ютерів (new hardware platforms and architectures); ігри та машинна творчість.

Як вже було сказано, інформаційні технології, в тому числі аналітико-статистичні технології, отримують своє практичне втілення у формі інформаційної системи, що об'єднує в собі як технічні засоби (комп'ютери, засоби та канали зв'язку, периферійні пристрої, пристрої введення/виводу даних тощо), так і програмні застосунки, що забезпечують функціонування технічної частини та аналітичну складову, включаючи математичну складову (статистику).

Питання функціонування аналітико-статистичних систем було досліджено Г. Бліновою. Для опису стану речей авторка використовує два терміни – інформаційна система та система інформаційного забезпечення. Система інформаційного забезпечення – це «система суспільних відносин, що виникають між різними суб'єктами з приводу обігу інформації, що здійснюється різними методами та за допомогою різних засобів» (Блінова, 2019, с. 138). В той час як інформаційна система – це елемент системи інформаційного забезпечення. У поєднанні із суб'єктами аналітичної діяльності в рамках держави система інформаційного забезпечення є, в широкому значенні, «сукупністю адміністративних правовідносин, що виникають між суб'єктами публічного та приватного права у процесі обігу інформації та задоволення їх інформаційних потреб (інтересів), обумовлених виконанням ними визначених законодавством завдань та функцій» (Блінова, 2019, с. 139). У вузькому – це «частина

управлінської діяльності з аналізу, планування і підготовки управлінських рішень, в безперервному процесі обробки та використання інформації про стан функціонування системи…», «що здійснюється за допомогою інформаційних засобів та методів, наслідком якої є формування інформаційних ресурсів та яка спрямована на забезпечення належного функціонування» (Блінова, 2019, с. 139).

В сучасних умовах цифрові технології двояко впливають на розвиток суспільно-економічних процесів. З одного боку, цифрові технології можуть бути загрозою, з іншого боку – інструментом захисту (Хамига, 2020, с. 68). Як підкреслює О. Юрченко, належне інформаційне забезпечення створює низку суттєвих переваг у сфері антикорупційної діяльності. Зокрема, воно сприяє підвищенню ефективності управління в державних органах, зменшує вплив суб'єктивних факторів на прийняття рішень у боротьбі з корупцією та забезпечує постійний моніторинг законності дій державних службовців. Крім того, розширене використання електронних баз даних дозволяє оперативніше ідентифікувати правопорушників, раціональніше розміщувати ресурси для боротьби зі злочинністю, налагоджувати міжвідомчу співпрацю під час розслідувань та забезпечує вищу якість підготовки підзаконних нормативно-правових актів (Юрченко, 2013, с. 84-85).

Залучення аналітико-статистичних технологій як інструменту попередження / протидії корупції на державному рівні обумовлено специфікою процесу ідентифікації корупції. Застосування відповідних технологій можливе за умов сприйняття корупції як виду шахрайства. Тому вважаємо за доцільне використати підхід Н. Ковтун (Ковтун, 2011, с. 14), згідно з яким пошук корупції в сучасних умовах розвитку суспільства необхідно здійснювати на основі комплексного використання математичних, аналітичних та психофізичних методів дослідження, що дасть змогу не лише ідентифікувати, але й прогнозувати ймовірні випадки.

До математичних методів ідентифікації корупції, в першу чергу, відносять застосування так званого закону Бенфорда у тестах Нигрини і Миттермайера у 1997 році, які було використані компанією «Ернст і Янг» під час проведення

аудиторських перевірок. Суть тесту полягає в тому, що «якщо внаслідок дослідження і побудови послідовності цифр емпіричних даних виявлені значні розбіжності з еталонними значеннями, то це є сигналом на проведення спеціального дослідження, яке виявить причину появи таких розбіжностей» (Ковтун, 2011, с. 14). Такі тести можуть бути застосовані при проведенні внутрішніх розслідувань, аудиті, податкових перевірках, оцінці тощо та дозволяють отримувати додаткові підтвердження щодо наявності / відсутності корупційної / шахрайської складової, навмисних / ненавмисних помилок в діяльності співробітників, контрагентів, організацій, підприємств тощо. Єдиною умовою ефективного застосування математичних методів є необхідність наявності значних масивів даних, тому для організацій з неінтенсивною операційною діяльністю вони не підходять. Тому більш розвинутими в плані можливостей ідентифікації корупційної / шахрайської активності є аналітико-статистичні методи. Ця група методів умовно поділяється на традиційну та автоматизовану групи (Ковтун, 2011).

До традиційних відносяться такі методи:

1. Метод пов’язаних зіставлень. Згідно з цим методом, будь-яка штучна (шахрайська, корупційна) подія порушує взаємозв’язки між зв’язаними показниками та не відповідає природньому стану речей. Так, наприклад, показники споживання електричної енергії можуть не відповідати показникам випуску продукції, розмір прибутку обсягу виробництва, обсягу спожитої сировини і випуску продукції. Цей метод дозволив виявити численні факти приховування прибутків від оподаткування та відмивання грошей (Ковтун, 2011, с. 13).

2. Метод спеціальних розрахункових показників визначає аналітичні показники звітних даних або інших джерел інформації з метою зменшити або виключити вплив чинників, пов’язаних із злочинними діями за умови: 1) виділення такого показника, який обов’язково змінюється під впливом штучної (шахрайської, корупційної) події; 2) розрахувати значення цього показника за умов нормально працюючого підприємства. У разі виявлення

розриву між реальним (дійсним) і бажаним (еталонним) значеннями цього показника робиться висновок про ймовірність шахрайства / корупційного злочину (Ковтун, 2011, с. 13).

3. Метод стереотипів здійснює пошук нелогічних зв'язків між економічними показниками або так званих «стереотипів», що відображає особливість певного способу скоєння злочину. Метод заснований на підході, згідно з яким злочин (шахрайська або корупційна схема) – це певним чином організована сукупність дій, процесів, тому метою методу є пошук незвичайних залежностей між економічними показниками, що відбивають структуру і зв'язки злочинної дії, які у звичних умовах зустрічаються доволі рідко (Ковтун, 2011, с. 13).

4. Метод скорегованих показників. Цей метод передбачає процедури зіставлення економічних показників з чинниками зовнішнього середовища, наприклад, порівняння цін, тарифів, за якими реалізуються товари з середньо ринковими (Ковтун, 2011, с. 13).

Дані методи відносяться до традиційних саме з того приводу, що розрахунки можливо зробити «на пальцях», на калькуляторі, принаймні у застосунку електронних таблиць (Excel, Google Tables тощо).

Їхньої протилежністю є методи, реалізація яких неможлива навіть в умовах використання зведених таблиць – автоматизовані аналітико-статистичні методи. Першою особливістю даних методів є допустимий розмір масиву даних. Так, наприклад, при використанні традиційного методу із застосуванням штатних засобів Microsoft Excel (без використання функції PowerQuery) користувач автоматично обмежений у кількості можливих записів в одній таблиці в 1 048 576 строчок ("Excel Specifications and Limits,"), в той час як автоматизовані аналітичні методи розраховані на обробку значно більшої кількості значень, для чого використовуються, наприклад, технології баз даних та відповідного до них середовища / мови обробки даних (S, R, Python, SQL), реалізовані, як на умовах вільної ліцензії (R, Python), так і умовно-безплатних (SPSS, SAS, SAP, Power BI). Застосування додаткових технологій дозволяє автоматизувати процес збору

первинної інформації (наприклад, за допомогою технологій розпізнавання образів автоматизується процес введення даних соціально-економічних та політичних досліджень), чищення (обробки) масивів даних (застосування логіки умовних виразів або технології машинного навчання). Другою перевагою цієї групи методів є можливість використання алгоритмів пошуку аномалій (викидів, новизни). Саме ці алгоритми стали розповсюдженими (впровадженими) в системах ідентифікації вторгнення, ідентифікації шахрайства / корупції, моніторингу здоров'я, виявлення електоральних аномалій, пошуку інсайдерів на біржі, сейсмологія тощо. Серед найпоширеніших алгоритмів виявлення аномалій виділяють такі: статистичні випробування, модельний тест, ітераційний алгоритм, метричний алгоритм, машинне навчання, ансамбль алгоритмів (Han, Hu, Huang, Jiang, & Zhao, 2022). Огляд сутності зазначених методів, як і специфіка їх використання будуть розглянуті у наступному підрозділі.

Нарешті, останнім засобом пошуку шахрайства / корупції є психофізіологічні методи, загальну характеристику яких було проілюстровано у таких серіалах як «Доктор Хаус» ("House MD," 2004-2012) або «Менталіст» ("The Mentalist," 2008-2015). Але найбільшої популярності вони отримали завдяки серіалу «Теорія брехні» ("Lie to Me," 2011-2013), за сценарієм якого теоретичні наробки в психології було органічно поєднано із передовими інформаційними технологіями (технологіями розпізнання образів), що дозволяють головному герою (доктору Лайтману) розслідувати заплутані та складні кримінальні та/або адміністративні справи. Хоча більшість сценаріїв – це вигадка або припущення, однак всі вони засновані на реальних можливостях сучасних комп'ютерів, що використовуються для автоматизації процесу протидії перевищенню швидкості, пошуку потенційних терористів в аеропортах та ін.

Основними напрямами оптимізації управління в організаціях, підприємствах, установах, галузях виробництва, державі загалом є підвищення його продуктивності та скорочення трудомісткості управління шляхом усунення втрат робочого часу та поєднання функцій, розвитку функціонального поділу праці, механізації та автоматизації управлінської праці, удосконалення

виробничої та організаційної структури, скорочення документації та раціоналізації документообігу. Основний напрямок підвищення ефективності управління виробництвом – автоматизація роботи з інформацією. Для автоматизації процесів збирання, обробки, передачі та збереження інформації, видачі її при необхідності для вирішення виробничих завдань створюють так звані автоматизовані системи управління виробництвом (АСУ). Розробка та застосування АСУ – один з найважливіших шляхів удосконалення управління та керівництва суспільним виробництвом ("Автоматизація виробничого підприємства : Системи управління виробництвом,").

Не лишилася осторонь і сфера попередження / протидії корупції, яка набула розмірів цілої галузі виробництва інформації, включаючи елементи розвідувальної, нормотворчої, організаційної та технологічної діяльності. Протидія зловживанню та правопорушенням на робочому місці мають безпосереднє відношення до суто управлінської задачі, змістом якої є не лише формулювання норм, процедур діяльності посадових осіб, а в першу чергу процеси розслідування будь-яких невизначених або аномальних ситуацій, що мають у собі ознаки навмисного спотворення звітної (контрольної) документації. Під час розслідувань фахівці намагаються знайти якомога більше доказів, як для належної та беззаперечної класифікації події (як випадкової ситуації, як зловживання на робочому місці, як умисного правопорушення (шахрайства) або умисного правопорушення зі змовою (корупція)), так і визначення кола підозрюваних або винуватих осіб. На сучасному етапі розвитку інформаційних технологій, їх застосуванні під час реалізації шахрайських / корупційних схем, фахівцям з протидії також доводиться озброюватися відповідним спорядженням – здійснювати автоматизацію своєї розвідувальної діяльності.

Якщо звернутися до досліджень, пов’язаних із попередженням / протидією корупції засобами інформаційних технологій, то більшість з них концентрує увагу на таких напрямках, як:

– цифрові державні послуги та електронний уряд;
– краудсорсингові платформи;

– інструменти інформування;
– портали прозорості та великі дані;
– технології розподіленої бухгалтерської книги (DLT) та blockchain;
– штучний інтелект (artificial intelligence) (Adam & Fazekas, 2018).

Досвіду української держави по створенню і реалізації відповідних цифрових інструментів показує, що він відповідає більшості зазначених напрямків.

Першим антикорупційним цифровим рішенням на державному рівні вважається система Prozorro, створена в 2014 році. Вона стала інструментом для проведення публічних закупівель, що дозволило кожному бажаючому спостерігати за етапами тендерів – від оголошення до укладання договорів ("Prozorro,").

У 2015 році з'явилася ініціатива Dozorro, започаткована Transparency International Україна. Ця платформа стала логічним продовженням Prozorro, сфокусувавшись на громадському моніторингу закупівель. Сервіс дозволяє користувачам оцінювати тендери, повідомляти про порушення, аналізувати ризики та впливати на ухвалення рішень ("Dozorro - громадський контроль держзакупівель,").

У 2016 році стартував сервіс Opendatabot, який також швидко завоював популярність серед бізнесу, юристів, журналістів та активістів. Він надає автоматичний доступ до численних державних реєстрів, включаючи судові рішення, податкові борги, зміни у компаніях, санкційні списки ("Opendatabot,").

Аналогічним за функціоналом можна вважати сервіс YouControl, що також надає інструментарій для перевірки компаній, бізнес-розвідки, аналізу ринків та візуалізації афілійованих зв'язків. YouControl інтегрує понад 50 державних джерел, дозволяючи формувати повне досьє на будь-якого контрагента чи фізичну особу ("YouControl : Перевіряйте контрагентів та стежте за їх змінами").

Інструментами Opendatabot та YouControl активно користуються представниками правоохоронних органів, журналістами та бізнесом для попередження шахрайства, аналізу ризиків і викриття корупційних схем.

У 2018 році було запущено державний портал Open Budget, розроблений Міністерством фінансів України. Цей ресурс дає можливість зацікавленим особам аналізувати доходи й витрати державного бюджету, відстежувати виконання бюджетних програм, а також оцінювати ефективність витрачання коштів як на національному, так і місцевому рівнях. Open Budget виконує дві важливі функції: підвищує прозорість бюджетного процесу та залучає громадян до обговорення фінансової політики ("Державний веб-портал бюджету для громадян"). Його наявність допомагає зменшувати ризики прихованих витрат, маніпуляцій та неефективних витрат.

На нашу думку, розглядати процес впровадження інноваційних аналітико-статистичних технологій необхідно за функціональними напрямками, тобто, з точки зору кінцевих продуктів (інформаційних систем, інформаційних середовищ), застосування яких тим або інших чином може сприяти меті попередження / протидії корупції в державі. З цього приводу можна виділити щонайменше п’ять функціональних напрямів автоматизації управлінської діяльності загалом, та антикорупційної діяльності зокрема:

1) автоматизація процесу збору та обробки даних;
2) автоматизація процесів комунікації (офісу);
3) автоматизація безпосередньо процесів управління;
4) автоматизація процесу розробки та прийняття управлінських рішень;
5) розвиток експертних систем.

Аналітико-статистичні технології отримують свої впровадження найбільше у чотирьох з визначених напрямів: збору / обробки даних; безпосереднього управління; підтримки прийняття рішень та експертній підтримці. Однак ми розглянемо всі зазначені функціональні напрямки в порядку ієрархії та масштабу (рівня) впровадження у розділі 3.

Отже, аналітико-статистичні технології мають не просто прикладне значення, а є ключовим елементом сучасного управління, особливо у сфері попередження / протидії корупції. На відміну від загальних інформаційних технологій, вони орієнтовані на глибокий аналіз, інтерпретацію та

прогнозування даних, що дає змогу державі, бізнесу й громадянському суспільству не лише реагувати на вже наявні проблеми, а й проактивно виявляти ризики й слабкі місця. Змістова характеристика зазначених технологій показує, що вони мають багаторівневу структуру та можуть охоплювати як прості аналітичні завдання (підготовка звітності), так і складні сценарії моделювання поведінки систем.

Ці технології стають важливим засобом не лише для державного управління, але й для всіх стейкхолдерів, зацікавлених у прозорості процесів. Вони слугують механізмом, через який дані перетворюються на інструменти впливу – як у внутрішньодержавному, так і в міжнародному вимірі. Це надзвичайно важливо в умовах високих ризиків, що супроводжують процеси реформування (цифровізації) державного сектора.

Тому саме держава має формувати запити на подібні аналітичні інструменти і бути головним замовником технологій моніторингу, виявлення й запобігання корупції. Без розуміння інституційного контексту застосування таких технологій (а це стосується як державної волі, так і технічної спроможності) неможливо правильно оцінити їхній потенціал. Ми бачимо, що аналітико-статистичні технології стають містком, який з'єднує управлінську функцію держави з практичними механізмами виявлення корупційних загроз.

2.3. Аналітико-статистичні підходи до виявлення корупційних загроз в інформаційних системах держави

1. Цифрова держава

Організації, в тому числі державні, що використовують власні чи спеціально розроблені для них інформаційні (корпоративні) платформи у своїй діяльності, можна умовно назвати цифровими. Додатково до інформаційної платформи, такі організації також можуть використовувати мобільні робочі місця, хмарні сервіси з управління персоналом, бухгалтерію і тому подібне, просувати свої товари та послуги в Інтернеті, здійснювати транзакції щодо продажу своїх продуктів / послуг онлайн. Цифрові організації можуть бути

представлені в будь-якій галузі економіки: фінансовій, нафтовій, енергетичній, транспортній, зв’язку тощо. І з кожним роком їх чисельність зростає, що призводить до появи вже цифрових урядів та держав. Як відомо, ідея переводу уряду в режим онлайн з’явилася ще в 1997 році в Естонії (Lufkin, 2017). Пройшло майже 20 років і в Україні з’явився проект «Держава у смартфоні» із застосунком ДІЯ (Хорішко, 2024, с. 605), що призвело до того, що у 2021 році саме Україна стала першою країною у світі ("Українці найбільше довіряють програмі «Держава у смартфоні» та цифровізації - опитування «Рейтинг»," 2021), яка на законодавчому рівні ввела електронні паспорти на рівні із паперовими. Крім цього, сервіс дозволив використовувати на рівні із паперовими аналогами водійські посвідчення, свідоцтва про народження, оформлення права на користування автотранспортним засобом та навіть сертифікати про вакцинацію проти COVID-19, а с початку введення воєнного стану ДІЯ почала застосовуватись як аналог посвідчення особи ("єДокумент – новий тимчасовий цифровий документ на період воєнного стану," 2022).

Свого часу дослідники І. Адам і М. Фазекас (Adam & Fazekas, 2018) проаналізували напрями або підходи до технологічного протистояння феномену корупції, а саме: 1) цифрові державні послуги та електронний уряд; 2) краудсорсингові платформи; 3) інструменти інформування; 4) портали прозорості та великі дані; 5) технології розподіленої бухгалтерської книги (DLT) та blockchain; 6) штучний інтелект (AI).

Щодо першого напряму автори стверджують, що цифрова трансформація державних послуг зменшує кількість прямих контактів між громадянами та чиновниками, а значить і зменшує ймовірність корупції. Цьому також сприяє поступова автоматизація фінансових операцій та публічність урядової діяльності. Разом це призводить до того, що цифрові державні послуги розширюють доступ до інформації, підвищуються прозорість та підзвітність уряду, зменшуючи тим самим ризик корупції та підриваючи можливості її впровадження. Незважаючи на емпіричне підтвердження статистичної залежності між показниками цифровізації державі та рівнем корупції, існують

негативні впливи цифровізації на анти-корупційну діяльність, що залежить від якості розвитку та впровадження відповідних проектів.

Наступним напрямом виявлення корупції є розробка інструментів зворотного зв'язку – як між громадянами і державною (crowdsourcing), так і між державними службовцями і державою (whistleblowing). Краудсорсингові та whistleblowing-платформи дозволяють громадянам і державним службовцям повідомляти про корупцію та публічно обмінюватися особистим досвідом. Ці платформи призначені для звітів про випадки як дрібної корупції, так і значно більшої корупції в державному секторі. Ефективність такого інструменту може бути забезпечена за допомогою простоти використання, гарантії анонімності, поширення застосування таких платформ та дій, що слідують після звернення громадян. Технологічний дизайн таких платформ повинен забезпечити захист IP-адрес заявників та передачу даних із врахуванням юридичних обмежень. Однак запровадження систем інформування може призвести до того, що корумповані чиновники знайдуть більш складні способи приховати правопорушення.

Четвертий напрям стосується розвитку порталів прозорості та використання великих даних у сфері антикорупційної діяльності. Портали прозорості – це спеціалізовані вебресурси, що забезпечують публічний доступ до масивів урядових даних, зокрема даних про державні закупівлі, розподіл бюджетних коштів, державну статистику, результати аудитів, реєстри прав власності, ліцензії, дозволи тощо. Такий доступ дозволяє не лише громадськості, а й журналістам-розслідувачам, неурядовим організаціям, дослідникам проводити незалежний моніторинг державної діяльності, виявляти системні корупційні ризики, а також забезпечувати підзвітність владних структур.

Важливим аспектом цього напряму є інтеграція принципів відкритих даних, що передбачає не лише оприлюднення інформації, а й її технічну придатність для автоматизованої обробки. Це створює передумови для застосування аналітико-статистичних технологій на рівні аналізу великих даних – наприклад, для виявлення закономірностей, трендів, аномалій у бюджетних витратах чи держзамовленнях. Використання великих даних

дозволяє значно підвищити ефективність антикорупційних зусиль, адже аналіз охоплює не окремі випадки, а системні зв'язки між структурами, транзакціями, контрактами, що відкриває нові горизонти для прогнозування та попередження корупційних схем.

Попри очевидні переваги, порталам прозорості властиві й певні обмеження. Зокрема, ефективність їхньої роботи прямо залежить від повноти, точності та актуальності завантажених даних, а також від наявності законодавчих механізмів, які зобов'язують органи влади надавати й оновлювати інформацію. Брак гармонізованих стандартів подання даних або відсутність політичної волі до реального забезпечення прозорості може звести нанівець навіть найкращі технологічні рішення. Однак у поєднанні з аналітико-статистичними підходами ці портали створюють потужний інструмент для боротьби з корупцією на макрорівні, роблячи публічне управління більш підзвітним і відкритим.

Blockchain як один із типів технології розподіленої бухгалтерської книги – це децентралізована та синхронізована база даних, що підтримується одноранговою мережею. Вся інформація (наприклад, транзакції) передається, перевіряється та зберігається в розподіленому регістрі як блоки інформації, які неможливо змінити або видалити. Тому створюються постійні та захищені записи, які можна використовувати. Блокчейн може бути використаний для управління інформаційним ланцюгом постачання, забезпечуючи повну прозорість. Він може застосовуватися урядом для державних операцій та документів, наприклад, для відстеження витрат на бюджет, збереження записів та реєстрів компаній або зміни системи контрактів та платежів. Система blockchain дозволяє забезпечити безпечне зберігання даних, запобігти можливості зламу та шахрайству та підвищити контроль та підзвітність. Сила блокчейна – це неможливість коригувати інформацію вручну для приховування дійсної ситуації. Однак залишається питання про те, яка частина такої інформації може бути представлена в повному обсязі для цілей громадського контролю без задіяння шкоди державі. Нейронні мережі можуть слугувати інструментом для

виявлення прихованих зв’язків за допомогою аналізу структури даних. Одним із інструментів нейронної мережі є самоорганізаційна карта (алгоритм нейронної мережі, що виконує завдання візуалізації та кластеризації), яка може витягувати шаблони з великих масивів даних. Цей інструмент може бути серйозною перешкодою для розвитку корупції. Однак якість таких технологій безпосередньо залежить від даних, на яких вони ґрунтуються. Нарешті два напрями функціонують разом – портали відкритих даних та штучний інтелект, за розвитком якого людство почало активно слідкувати з початку презентації проекту OpenAI та його продукту ChatGPT.

Виходячи з цих напрямків, процес розвитку інформаційних технологій у сфері боротьби з корупцією можна поділити на кілька етапів:

1. Етап «цифровізації» – на цьому етапі інформаційні технології були введені у сферу боротьби з корупцією як засіб автоматизації процесів введення даних. Наприклад, запровадження електронних баз даних, електронного документообігу та електронної звітності.

2. Етап «відкритих даних» – на цьому етапі були створені платформи для публічного доступу до даних про державні закупівлі, бюджетні витрати, доходи та майно посадових осіб тощо. Це дозволило громадянам та журналістам легше відслідковувати та виявляти випадки корупції.

3. Етап «цифрової ідентифікації» – на цьому етапі було впроваджено засоби та технології для електронної ідентифікації громадян та посадових осіб, що дозволяє підвищити прозорість та відстежуваність державних процесів.

4. Етап «штучного інтелекту та аналітики» – на даному етапі відбувається широке впровадження систем і технологій аналітики даних та штучного інтелекту, що дозволяє більш ефективно виявляти та запобігати випадкам корупції, наприклад, за рахунок аналізу великих обсягів даних та виявлення аномалій у поведінці посадових осіб та державних структур.

5. Етап «цифрової економіки та блокчейн» – на даному етапі активно розвиваються блокчейн-технології, які дозволяють забезпечити надійний захист

від підробок, маніпуляцій та фальсифікацій, включаючи документообіг, електронні голосування та інші процеси, пов'язані з боротьбою з корупцією.

Ці етапи є умовними та можуть перегукуватись один з одним. Вони можуть різнитися у різних країнах, залежно від рівня розвитку інформаційних технологій і соціально-політичних особливостей. Ми бачимо, що аналітико-статистичні технології мають безпосереднє відношення до четвертого етапу та межують з п’ятим – етапом, що має безпосереднє відношення до теми безпеки в цифровому середовищі. Проникнення інформаційних технологій, з одного боку, дає цифровим організаціям, підприємствам та установам перевагу у швидкості надання послуг, їх якості та ціні тощо, але з іншого боку, зростають ризики кібербезпеки.

2. Пошук внутрішніх загроз як основа попередження корупції

Для мінімізації ризиків кібербезпеки застосовують різноманітні технічні рішення. Найбільш повний перелік інноваційних аналітико-статистичних технологій, а точніше виробників подібних систем можна знайти тут ("CYBERscape," 2022), що розподілений за 12 напрямками:

– безпека мереж та інфраструктури (network & infrastructure security);
– моніторинг та адміністрування інструментів захисту інформації;
– управління ідентифікацією та доступом (identity & access management);
– веб-безпека (web security);
– безпека даних (data security);
– реагування на інциденти та заходи безпеки (security ops & incident response);
– розвідка загроз (threat intelligence);
– управління цифровими ризиками (digital risk management);
– безпека блокчейн (blockchain);
– захист кінцевих точок (endpoint security);
– безпека застосунків (application security);
– безпека мобільних пристроїв (mobile security);
– інтернет речей (IoT);

– безпека засобів комунікації (messaging security);

– послуги та консультації з питань безпеки (security consulting & services);

– безпека транзакцій та захист від шахрайства (fraud & transaction security);

– хмарна безпека (cloud security);

– ризик і комплаєнс (risk & compliance).

Однак, проблема полягає в тому, що існуючі інформаційно-технічні засоби ефективно захищають від зовнішніх загроз (DDOS-атаки, підбір паролів, обхід мережевих екранів, зараження вірусами), в той час як корупція є внутрішньою загрозою. В контексті нашого дослідження ми маємо справу із питанням захисту інтересів державних організацій (будь-то звичайна комунальна компанія чи орган державної влади) від внутрішнього зловмисника (корупціонера, шахрая), для якого в інформаційній науці було запозичено англомовний термін «інсайдер» (від англ. “insider”) – «особа, яка завдяки своєму службовому становищу або спорідненим зв’язкам має доступ до конфіденційної інформації … , що недоступна широкій громадськості, та може використати її у власних цілях з метою збагачення, одержання неконкурентних переваг, привілеїв тощо» (*Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції*, 2018, с. 312).

Інсайдерами можуть бути: 1) фізичні особи (власники істотної участі, управлінський персонал (персонал із статусом ОПР, працівники внутрішнього аудиту, члени ревізійної комісії, контролери), асоційовані особи (рідні брати, сестри, батьки, чоловік, дружина або повнолітні діти керівників, контролерів організації та акціонерів-власників істотної участі (від 10%)); 2) юридичні особи (власники істотної участі, афілійовані, споріднені особи та асоційовані особи.

В свою чергу, наявність інсайдерів створює інсайдерські (внутрішні) загрози – шкідливі для соціальної системи активності, які походять від її елементів, зокрема – від діючих працівників, колишніх працівників, підрядників,

ділових партнерів і навіть завербованих працівників або працівників, навмисно впроваджених в організацію, які мають доступ до конфіденційної інформації в рамках своїх посадових обов'язків та які мають уявлення про систему управління інформаційною безпекою організації (Predd, Pfleeger, Hunker, & Bulford, 2010, p. 170).

Саме через наявність адекватних засобів захисту від зовнішніх атак, значними витратами на їх здійснення, більш економічно вигідним є використання інсайдерів, які можуть не тільки, наприклад, своїми руками чи руками колег несанкціоновано вивантажити конфіденційну інформацію на власний носій, переслати через електронну пошту, вилучити зашифрований жорсткий диск з робочої станції або сервера тощо, але й можуть провести низку легальних процедур щодо виведення інформації із захищених контурів та сховищ за рахунок використання власних посадових повноважень та мережевих привілеїв. Найбільшу цінність для інсайдера становлять об’єкти концентрації даних – сховища.

На нашу думку, найбільш дотичними до проблеми попередження / протидії корупції є інструменти з реагування на інциденти та засоби безпеки та оцінки ризику і комплаєнсу. Застосунки з реагування на інциденти та заходи безпеки поділяються на:

– управління інформацією про безпеку та події безпеки (security information and event management)

– реагування на інциденти безпеки (security incident response)

– аналіз безпек (security analytics).

В свою чергу ризик і комплаєнс поділяється на рішення з:

– оцінки та візуалізація ризиків;

– вимірювання ризику;

– симуляції атак та взломів (BAS – breach and attack simulation);

– врядування, управління ризиками та дотримання вимог законодавства (GRS – governance, risk management and compliance);

– освіти з питань інформаційної безпеки.

Таким чином, інноваційними аналітико-статистичними технологіями, що можуть бути використані у корпоративних системах моніторингу, попередження та протидії корупції в державі можна вважати ті технології, що сфокусовані на пошуку ознак аномальної (зловмисної) активності користувачів у великих масивах даних, що відображають результати діяльності публічних (урядових) організацій, підприємств та установ. Ці інформаційні масиви формуються з трьох джерел:

– даних, що характеризують основну господарську діяльність органів публічної влади, в тому числі дані постійного моніторингу режиму їх роботи;

– персональних даних співробітників органів публічної влади, які одночасно здійснюють свою активну професійну діяльність;

– дані щодо поточних операцій з клієнтами та контрагентами органів державної влади та місцевого самоврядування, що здійснюються зазначеними співробітниками в рамках виконання покладених на них посадових обов'язків.

В умовах становлення цифрової цивілізації для боротьби з внутрішніми зловмисниками інформаційних систем використовується ряд технічних засобів, таких як DLP (data loss prevention (запобігання втраті даних) або data leakage prevention (запобігання витоку даних)), SIEM (security information and event management – об'єднання двох термінів, що позначають використання програмного забезпечення: SIM (security information management) – управління інформацією про безпеку та SEM (security event management) – управління подіями безпеки) тощо. Але ці засоби проводять моніторинг нелегальних каналів, в той час як корупціонери чи фінансові шахраї використовують легальні канали руху інформації. Їх злочинні дії, прикриті діяльністю щодо виконання посадових обов'язків, з точки зору науки про інформацію класифікуються як інсайдерські атаки. Вони стають не тільки більш економічно вигідним способом злочинних дій в інформаційному просторі, а все частіше і єдиними можливими. В більшості випадків злочинні (корупційні, шахрайські) дії в умовах цифрової організації пов'язані із маніпуляціями чи махінаціями з інформацією – її крадіжкою, фальсифікацією чи банальним приховуванням.

Для пошуку ознак корупційної (інсайдерської) активності в масивах даних необхідно мати навички оперувати великими обсягами поточної інформації, аналізуючи її та формуючи рекомендації для прийняття відповідних управлінських рішень в умовах жорстких часових обмежень. Саме цим і обумовлено використання в подібному аналізі інноваційних аналітико-статистичних засобів, в тому числі, систем штучного інтелекту, за допомогою яких забезпечується інтелектуальний аналіз даних у відповідному часовому режимі. При цьому необхідно, щоб сформовані в процесі такого аналізу рекомендації були зрозумілі не лише експертам, а й керівникам відділів служб безпеки, що займаються як питаннями інформаційної безпеки, так і питаннями попередження / протидії шахрайству і корупції.

Таким чином, в умовах інформаційного простору, в тому числі цифрової держави, будь-яка особа, що зловживає своїм посадовим становищем з метою отримання власного зиску чи зиску для третіх сторонніх осіб, в контексті інформаційних систем протидії їй, відноситься до категорії інсайдерів.

Як зазначено в (Salem, Hershkop, & Stolfo, 2009, p. 70) інсайдери (точніше, зловмисні інсайдерські загрози) поділяються на дві групи: зрадників та маскувальників. Зрадники мають повне уявлення про системи, з якими вони працюють щодня, а також фактичну політику безпеки. Вони діють від свого імені, тому використовують власні повноваження для зловмисних дій. Маскувальники крадуть облікові дані інших законних користувачів, а потім використовують їх для здійснення зловмисної дії від імені «жертви».

Згідно з дослідженням (Cappelli, Moore, & Trzeciak, 2012, p. 3-5) інсайдерські загрози можна класифікувати за такими типами:

– IT-саботаж (sabotage), під час якого інсайдер використовує інформаційні технології для заподіяння конкретної шкоди організації чи фізичній особі;

– розкрадання інтелектуальної власності або так зване шпигунство (theft);

– шахрайство (fraud) – коли інсайдер використовує інформаційні технології для несанкціонованої зміни, додавання чи видалення даних організації для особистої вигоди чи крадіжки.

Для виявлення загроз будь-якого типу в інформаційних системах використовуються найновіші аналітико-статистичні технології, засновані на технології машинного навчання. Зміст таких технологій полягає в тому, щоб «навчити» інформаційну систему розпізнавати дії інсайдерів, для чого використовуються навчальні набори даних. В контексті нашої роботи, найбільш адекватним з точки зору виявлення шахраїв та корупціонерів, є набори даних, що схожі за своєю сутністю на набір даних Enron. Це набір даних славнозвісної компанії Enron (Cohen, 2015), що складається з 500 000 реальних електронних листів (з 1998 по 2002 рік), пов’язаних з 150 користувачами, переважно з вищим керівництвом корпорації Enron. Набір даних дозволяє створювати моделі для аналізу тексту в електронних листах та аналізу даних соціальних медіа, спрямованих на виявлення змови між учасниками комунікації.

Більшість практик та IT-технологій, які дозволяються виявити інсайдера, функціонують лише після вчинення злочину. Наприклад, система аудиту, в якій фіксується послідовність дій зловмисника, що спрощує розслідування інциденту. База даних скоєних злочинів може бути використана для підготовки системи моніторингу для формування системи показників ризику. З метою виявлення шахрайської чи корупційної активності співробітників на ранніх стадіях використовуються дані з багатьох джерел даних – кадрової бази даних, бази даних фізичного доступу до приміщень, бази даних доступу до інформаційних систем, ролі в інформаційних системах.

Саме тому значна увага в системах попередження / протидії шахрайським / корупційним діям увага зосереджена на виявленні аномальних «вторгнень»: зловмисного доступу до перегляду або редагування баз даних. Пошук аномалій здійснюється на основі порівняння дій користувачів із так званими поведінковими профілями (normative model of behavior) (M. I. Khan & Foley, 2016; M. I. Khan, Foley, & O'Sullivan, 2017). Вони можуть бути синтаксично,

контекстно та результативно (data) орієнтованими (Hussain, Sallam, & Bertino, 2015; Mathew, Petropoulos, Ngo, & Upadhyaya, 2010; Sallam, Fadolalkarim, Bertino, & Xiao, 2016) та можуть бути представлені як система виявлення аномалій Black-Box (незрозумілі для користувача) та White-Box (причину аномалії можуть ідентифікувати адміністратори (співробітник служби безпеки, адміністратор бази даних тощо) при перевірці аномалії). Остання передбачає, що система може допомогти пояснити аномалії, а отже систему можна вважати експертною.

3. Методи виявлення аномалій як індикаторів зловмисної (корупційної) діяльності

Аномалії можна вважати тими шаблонами в даних, що відхиляються від очікуваних. Зловмисники завжди намагаються пристосовувати свою поведінку таким чином, щоб вона виглядала адекватною (normal). При цьому зразок адекватності завжди залежить від умов середовища і знаходиться у концептуальному дрейфі – поточне поняття номінальної поведінки не може відображати номінальну поведінку в майбутньому (Gama, Žliobaitė, Bifet, Pechenizkiy, & Bouchachia, 2014, p. 3). Ускладнює проблему відсутність маркованих даних, необхідних для підготовки та перевірки моделі, та універсального детектору аномалій (Das, Wong, Fern, Dietterich, & Siddiqui, 2017).

Представимо найпопулярніші аналітико-статистичні методи виявлення аномалій.

1. Локальний коефіцієнт викиду (Local Outlier Factor – LOF) (Breunig, Kriegel, Ng, & Sander, 2000) – є найвідомішим алгоритмом для знаходження викидів на основі щільності і першим вводить поняття локального відхилення. Цей алгоритм присвоює ступінь відхилення кожній одиниці спостереження. Алгоритм є локальним в тому сенсі, що він розглядає тільки обмежене коло спостережень, що знаходяться поруч один з одним. Перевагою методу є те, що він може бути використаний для виявлення всіх видів відхилень, в тому числі тих, які не можуть бути виявлені алгоритмами на основі відстані (Ertoz et al., 2003). Метод погано працює з наборами даних, що містять глобальні аномалії,

породжуючи багато помилкових результатів. Цей метод не призначений для виявлення ознак змови (корупції) (Goldstein & Uchida, 2016).

2. Об’єднання в кластери або кластеризація – зазвичай здійснюється неконтрольованим або напівконтрольованим способом. У першому підході модель проходить навчання з використанням як номінальних, так і аномальних даних. За умов напівконтрольованого способу модель проходить навчання з використанням тільки номінальних даних. Після чого модель використовується як профіль, що описує номінальну поведінку (Bhuyan, Bhattacharyya, & Kalita, 2014). Існує багато способів кластеризації:

– евклідова відстань;

– відстань Махаланобіса (Mimmack, Mason, & Galpin, 2001);

– K-means (Kumari, Sheetanshu, Singh, Jha, & Singh, 2016);

– метод опорних векторів або опорно-векторних мереж (SVM – support vector machine) та його варіації (Erfani, Rajasegarar, Karunasekera, & Leckie, 2016);

– метод ансамбля (Das, Islam, Jayakodi, & Doppa, 2019), варіацією якого є метод iForest (Shao, Du, Yu, & Chen, 2022), що є алгоритмом дерева рішень на основі ансамблю для виявлення неконтрольованих аномалій. Цей метод припускає, що аномалії знаходяться в меншості і що їх значення дуже відрізняються від номінальних екземплярів. Метод будує колекцію ізольованих дерев для заданого набору даних, а потім трактує як аномальні ті спостереження, що перевищують середню довжину шляху (J. Chen, Zhang, Qian, Yuan, & Ren, 2023).

Щоб подолати труднощі при аналізі багатовимірних, гетерогенних даних, деякі дослідники зосередилися свою увагу на алгоритмах машинного навчання та теорії графів. Для виявлення аномалій у моделях графів можна виділити такі підходи.

1. Пошук інсайдерських загроз в сумісних інформаційних системах (CADS – community-based anomaly detection system) (Y. Chen & Malin, 2011), де система виявлення аномалій запропонованої інфраструктури виявляє

найближчих сусідів кожного користувача і обчислює відхилення кожного користувача від своїх найближчих сусідів.

2. Пошук текстових аномалій (Eberle & Holder, 2009), що можна використовувати для аналізу бази електронної пошти або повідомлень (дзвінків).

3. Система виявлення внутрішніх загроз (Brdiczka et al., 2012), що використовує графічне навчання та психологічне моделювання користувачів.

4. Метод пошуку аномалій, що використовує теорію графів для створення графів знань і графів залежностей об'єктів (Althebyan & Panda, 2007). Граф знань представляє одиниці знань для даного користувача, які оновлюються з часом. Граф залежності – це глобальний ієрархічний граф, що показує всі залежності між різними об'єктами (Althebyan & Panda, 2007, p. 242-243).

5. Метод маркованих графів, в якому вузли і ребра демонструють свої властивості як через топологію графа, так і через атрибути графа (Ma et al., 2022). Методи виявлення аномалій у маркованих графах можна розділити на структурні (structure-based) та групові (community-based). Основна ідея структурних методів полягає в ідентифікації незвичайних підструктур, заснованих на зв'язності графів, а також атрибутів. Знаходження на основі спільності аномалій у маркованих графах більше підходить для виявлення шахрайської / корупційної загрози, оскільки дозволяє проаналізувати індивідуальну поведінку людей по відношенню до своїх колег. Серед робіт у цьому напрямку також можна виділити метод Zhou (Zhou, Cheng, & Yu, 2009), Moser (Moser, Colak, Rafiey, & Ester, 2009), Gunnemann (Gunnemann, Boden, Farber, & Seidl, 2013), Liu (G. Liu & Wong, 2008).

6. Методи ранжування відхилень в графах: CODA (Gao et al., 2010), FOCUSCO (Perozzi, Akoglu, Iglesias Sánchez, & Müller, 2014), GOutRank (Muller, Sanchez, Mulle, & Bohm, 2013).

Загалом, сучасні підходи до виявлення шахрайських / корупційних загроз базуються на методах криміналістики (forensic) і зазвичай обмежують себе вивченням журналів кібербезпеки для застосування алгоритмів виявлення аномалій або пошуку відбитків (сигнатур). Ці алгоритми необхідні для виявлення загрози, але вони лише є складовою повного рішення. Тому більш

ефективними слід вважати інтегровані рішення з виявлення та запобігання шахрайству / корупції, що використовують семантично марковані дані з інфраструктури кібернетичного та фізичного контролю доступу і забезпечують проактивне, упереджене виявлення зловмисників.

В контексті попередження / протидії корупції, система пошуку аномалій має зосереджуватися на пошуку особливих аномалій, які називаються змовою. Наприклад, збір цінної інформації працівниками з використанням особистих відносин є серйозною проблемою інформаційної безпеки в урядових і комерційних організаціях. У цьому випадку часто порушник інформаційної безпеки має доступ до частини цінної інформації, але не має права на її отримання повністю. Прикладом такої ситуації може бути поділ спільної проблеми на різні підрозділи організації. Тоді інсайдер буде намагатися отримати відсутню інформацію у своїх друзів з інших підрозділів або піти на змову щодо збору та подальшого продажу цінної інформації.

Отже, ми дійшли до розуміння того, що аналітико-статистичні підходи до виявлення корупційних загроз у державних інформаційних системах формуються на основі багатокомпонентної цифрової архітектури, яка охоплює різні рівні: від цифрових державних послуг до штучного інтелекту й блокчейн-технологій.

Важливим етапом цифрової трансформації держави є розгортання систем зворотного зв’язку, таких як краудсорсингові й whistleblowing-платформи, що надають можливість громадянам і держслужбовцям анонімно повідомляти про порушення. Ці інструменти, хоч і ефективні в окремих кейсах, мають очевидні межі, зокрема, потребують комплексного технологічного дизайну для захисту даних та анонімності користувачів, а також реальної політичної волі для реагування на повідомлення.

Використання порталів прозорості створює умови для незалежного громадського моніторингу, але водночас ставить завдання якісного та повного наповнення інформаційних баз. Ефективність аналітико-статистичних технологій безпосередньо залежить від їх здатності працювати з великими

масивами даних, виявляти закономірності, тренди, аномалії – і таким чином перетворювати сирі дані на дієві антикорупційні інструменти. Однак недостатня стандартизація, неповнота даних чи затримки в оновленні інформації можуть істотно знижувати потенціал таких платформ.

Наріжним каменем сучасних технологій є впровадження блокчейн-рішень і штучного інтелекту, що дозволяють закладати в системи прозорості та безпеки принципи незмінності даних, автоматизованого моніторингу та навіть передбачувальної аналітики. Разом із тим, ми розуміємо, що будь-яка технологія, якою б просунутою вона не була, працює в реальному соціальному й політичному середовищі, де є ризики маніпуляцій, підтасовок і навіть використання легальних каналів для прикриття злочинної діяльності. Це означає, що технічні рішення потребують супроводу у вигляді нормативного, організаційного й етичного врегулювання.

Окремо ми звертаємо увагу на проблему інсайдерських загроз, які становлять головну складність у сфері інформаційної безпеки державних органів. На відміну від зовнішніх атак, дії інсайдерів часто виглядають як частина легальної роботи: це може бути як виведення інформації, так і фальсифікація даних, прикрита посадовими повноваженнями. Сучасні системи безпеки здатні виявляти лише порушення вже після факту злочину, тоді як справжній виклик полягає в розробці проактивних підходів, що дозволяють розпізнавати шахрайські або корупційні схеми на стадії їхнього формування.

Ми вважаємо, що особливо перспективними є системи, засновані на машинному навчанні, здатні аналізувати багатовимірні дані, формувати поведінкові профілі та виявляти аномалії, включаючи змови. Такий аналіз вимагає не лише технічних рішень, але й наявності відповідних даних (наприклад, кейси на кшталт відомого набору даних Enron), що дозволяють будувати алгоритми для реального середовища. Багато підходів у цьому полі, зокрема використання графових моделей чи методів кластеризації, орієнтуються на виявлення патернів взаємодії, що дає змогу ідентифікувати не тільки індивідуальних порушників, а й цілі групи, залучені в корупційні схеми.

Висновки до другого розділу

Узагальнюючи висновки другого розділу можна стверджувати, що держава є не лише майданчиком для виникнення корупційних практик, але й центральним актором у боротьбі з ними. Складність обумовлена багаторівневістю самої держави як інституційної системи, де поєднуються елементи публічної влади, корпоративного управління, політичної системи та неформальних зв'язків. Корупція не виникає у вакуумі – її ґенеза детермінована якістю інституцій, наявністю (або відсутністю) реальної конкуренції еліт, рівнем політичної відповідальності та механізмами контролю за владою. При цьому саме слабкість системи делегування повноважень і недостатній розподіл публічного та приватного інтересів стають ґрунтом для структурної корупції, коли сама держава перетворюється на інструмент приватних інтересів.

Навіть за умов слабкої політичної системи держава все ж залишається ключовим інструментом попередження / протидії корупції. Це можливо лише за наявності чітко визначених моделей антикорупційної політики, які враховують як інституційні, так і культурні, соціальні та економічні особливості. На жаль, універсального рішення не існує, а будь-які зусилля по впровадженню досвіду інших країн потребують глибокого розуміння національного контексту. Тому антикорупційна політика повинна бути комплексною, цілісною й системною, щоб мати шанс змінити правила гри за будь-яких форс-мажорних обставин, буть то пандемія або війна.

Аналіз змісту аналітико-статистичних технологій демонструє, що ці інструменти є не просто технічними рішеннями, а важливими компонентами цифрової трансформації державного управління. Ідея "держави як інформаційної платформи" стає центральною у сучасних уявленнях про реформування держави, а цифровізація сприймається як спосіб не лише зменшити адміністративні витрати, а й мінімізувати можливості для корупції шляхом скорочення прямих контактів між громадянами та чиновниками. При цьому саме аналітико-статистичні інструменти – від Big Data до штучного інтелекту –

стають ядром цього процесу, перетворюючи управлінську діяльність на орієнтовану на дані й сервіс.

Для ефективної роботи таких технологій потрібна не тільки технічна база, але й добре вибудувані організаційні, нормативні та управлінські рамки. Успішна антикорупціна політика за сучасних умов розвитку технологій має орієнтуватись на інтеграцію технологій у єдину цифрову платформу, що дозволяє уникнути дублювання функцій, зменшити фрагментацію даних і створити справді клієнтоорієнтовану державу. Адже, цифровізація – це не тільки про техніку, а й про культуру, мислення та нові підходи до взаємодії між державою, бізнесом і громадянами.

Аналіз існуючих аналітико-статистичних підходів до виявлення корупційних загроз в інформаційних системах держави визначив, що головною проблемою стають не стільки зовнішні атаки, скільки дії внутрішніх зловмисників – інсайдерів. Сучасні технічні засоби добре захищають системи від зовнішнього втручання, однак корупціонери діють із середини, використовуючи легальні канали та власні службові повноваження. Це потребує застосування складних інструментів, таких як системи аналізу поведінкових профілів, алгоритми виявлення аномалій, методи кластеризації й навіть елементи штучного інтелекту, які здатні працювати з великими масивами даних у режимі реального часу.

Тому, ефективна боротьба з корупцією всередині цифрових організацій можлива лише за умови інтеграції технічних, організаційних і поведінкових підходів. Однією з ключових проблем є не просто виявлення злочину постфактум, а запобігання йому на ранніх стадіях, що вимагає побудови систем моніторингу, здатних працювати проактивно. Лише комплексне використання аналітико-статистичних методів, адаптованих під специфіку кожної державної організації або органу місцевого самоврядування, може забезпечити реальне зниження ризиків. Зрештою, успішне впровадження таких систем потребує не лише інвестицій у технології, а й розвитку аналітичної культури серед управлінців і працівників служб безпеки.

РОЗДІЛ 3
ПРАКСЕОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ПРОБЛЕМИ ІННОВАЦІЙНИХ АНАЛІТИКО-СТАТИСТИЧНИХ ТЕХНОЛОГІЙ ПОПЕРЕДЖЕННЯ КОРУПЦІЇ В ДЕРЖАВІ

3.1. Функціональні напрями та технологічні платформи застосування аналітико-статистичних систем для попередження корупції

В цьому підрозділі розглянемо аналітико-статистичні технології в контексті забезпечення антикорупційної діяльності за визначеними у попередньому розділами функціональними напрямками.

1. Інформаційна технологія обробки даних.

Подібна технологія розробляється для вирішення добре структурованих проблем, згідно з якими відомі необхідні вхідні дані та алгоритми та інші стандартні процедури обробки. Технологія забезпечує автоматизацію збору оперативної інформації за всіма підрозділами організації, підприємства чи установи та зменшує кількість технічних помилок у зв’язку із людським фактором. Впровадження будь-якого варіанту цієї технології в діяльності організації обумовлена законодавчими нормативами, оскільки згідно із законом кожна юридична або фізична особа-підприємець мають зберігати певні дані, пов’язані із основним видом економічної діяльності, які можуть бути використані контролюючими органами або третіми особами під час аудиту чи контролю. Чим більш автоматизована систем, тим менше ймовірність навмисного спотворення даних, та ефективність виконання операцій з аудиту / контролю, як внутрішнього, так і зовнішнього.

Прикладом застосування відповідних технологій є як індивідуальні (текстові та табличні редактори, локальні системи управління базами даних з пакетів Apache OpenOffice, Apple iWork, Corel WordPerfect Office, LibreOffice, Microsoft Office, WPS Office, включаючи застосунки для роботи з pdf від Adobe, ABBYY, Foxit, Sumatra тощо) так і корпоративні інформаційні системи

(Salesforce, BAS, Microsoft Dynamics, Oracle E-Business Suite, SAP тощо), в тому числі хмарні застосунки на кшталт Google або Zoho.

2. Автоматизація процесів комунікації.

Ця технологія спочатку була впроваджена у виробничих процесах, а згодом набула поширення й у сфері управління, охопивши діяльність координаційних підрозділів і спрямовуючись передусім на автоматизацію рутинних завдань секретарського характеру. З розвитком комунікаційних засобів автоматизація офісних процедур почала привертати увагу управлінців і спеціалістів, які розглядали її як засіб підвищення продуктивності праці. При цьому її завданням не є витіснення традиційної системи комунікацій – з нарадами, телефонними розмовами й адміністративними розпорядженнями – а її раціональне доповнення.

В даний час відомо кілька десятків програмних продуктів для комп'ютерів та некомп'ютерних технічних засобів, що забезпечують технологію автоматизації офісу: текстовий процесор, табличний процесор, електронна пошта, електронний календар, аудіо- та відеоконференції, хмарні технології збереження даних (зображень, аудіо-, відео-записів), а також спеціалізовані програми управлінської діяльності: ведення документів, контролю за виконанням наказів тощо. За період впровадження карантинних обмежень у зв'язку із вірусом COVID-19, було автоматизовано майже увесь світ. Якщо раніше використання віддаленого формату роботи були притаманні лише фахівцям з інформаційних технологій або так званим віддаленим співробітникам, то зараз онлайн-зустріч є опцією за замовченням. Особливо затребуваною стала автоматизація офісної діяльності для України після 24 лютого 2022 року. Найголовнішою перевагою автоматизації офісу для фахівців з протидії корупції є те, що комунікація є однією із форм отримання інформації про скоєні корупційні злочини, в першу чергу це стосується опитування кола підозрюваних осіб. Системи віддаленої комунікації автоматизують процеси запису розмов із свідками, жертвами та учасниками та співучасниками правопорушень.

Що стосуються даного сегменту технологій, то тут маємо дуже розгалужений перелік застосунків, що включає в себе застосунки з попереднього пункту. Пропонуємо розділити наявні (найбільш популярні) застосунки за такими функціональними напрямами:

– створення / редагування текстових документів: Apache OpenOffice Writer, Apple Pages, Corel WordPerfect, Google Documents, LibreOffice Writer, Microsoft Office Word;

– створення / редагування таблиць: Apache OpenOffice Calc, Apple Numbers, Corel Quattro Pro, Google Tables, LibreOffice Calc, Microsoft Office Excel;

– створення / редагування баз даних: Apache OpenOffice Base, LibreOffice Base, Corel Paradox Database, Microsoft Office Access, в тому числі СУБД Oracle, SQL, Vusial FoxPro;

– обробка, аналіз та візуалізація даних: Jamovi, JASP, JMP (SAS), KNIME, Maple, MATLAB, MaxQDA, Pandas (Python), PSPP, R, RapidMiner (Altair), SAS, SPSS (IBM), Statistica, WPS (Altair);

– створення, редагування, заповнення електронних форм, розпізнавання тексту: Adobe Acrobat, ABBYY FineReader, Kofax OmniPage;

– персональні інформаційні системи та системи обміну електронними повідомленнями: Microsoft Outlook, Lotus Organizer, Lotus Notes, Apache Open Office Schedule, Google Suite, Zoho;

– створення / редагування презентаційних документів: Apache OpenOffice Impress, Apple KeyNote, Corel Presentations, Google Presentations, LibreOffice Impress, Microsoft Office PowerPoint;

– організація аудіо-, відео-конференцій: Google Meet, Microsoft Teams, Zoom;

– накопичення, зберігання та синхронізації даних: Amazon Drive, Apple iDrive, Dropbox, Google Drive, Microsoft OneDrive.

Список можна продовжувати застосунками для видавничої діяльності, створення растрової / векторної графіки, 3D-графіки тощо.

Зазначимо, що деякі функції комунікаційних інформаційних технологій можуть бути інтегровані в більшість корпоративних інформаційних системи: Salesforce, BAS, Microsoft Dynamics, Oracle E-Business Suite, SAP за умови додаткової оплати.

3. Інформаційна технологія управління.

Технологія впроваджується із метою задоволення інформаційних потреби всіх співробітників організації, підприємства чи установи, на яких покладено функцію ухвалення рішень. Ця технологія орієнтована на роботу з менш структурованими завданнями і може бути корисною на будь-якому рівні управління.

Зазначена інформаційна технологія дозволяє вирішувати завдання з оцінювання стану об’єкта управління; аналізу відхилень від запланованого стану; визначення причини відхилень (викидів, аномалій); аналізу подальших дій.

Реалізація даної технології передбачає залучення статистичного інструментарію не лише описової частини дисципліни, а й вивідної, в тому числі статистик центральної тенденції, мір розкиду, методі інтерполяції / екстраполяції і т.п. Активно залучаються інструменти з візуалізації даних. Починаючи з цього рівня впровадження інформаційних технологій говорять про їх групи, тобто виділяють (Kale, 2016):

– системи планування ресурсів (ERP) – орієнтовані на моніторинг господарських процесів, до яких відносяться складання планів та прогнозів, управління продажами, адміністрування випуску товарів, закупівель;

– системи взаємодії із замовниками (CRM) – розроблені для організації взаємовідносин з клієнтами (контрагентами), а також з діловими партнерами;

– системи адміністрування логістичних ланцюжків (SCM) – розробляються для процесів створення складних товарів, особливо в умовах, коли комплектуючі замовляються у різних постачальників, що дозволяє розраховувати та відстежувати постачання на всіх етапах;

– системи планування матеріальних потоків (MRP) – моніторинг придбання, виготовлення і реалізації продукції;

– системи управління кадровими ресурсами (HRM) – автоматизують роботу відділів кадрів, а також забезпечують пошук потенційних співробітників за наявними в базі даних резюме;

– системи підтримки аналітичної діяльності (BI) – призначені для обробки та аналізу даних.

Останньою, найголовнішою, характеристикою подібних систем є унікальність конфігурації системи для кожної організації навіть за умов наявності типових шаблонів. Тому значна сума витрат на ці застосунки складається не з виплат на ліцензії, а виплати за налаштування (впровадження) та підтримку актуальності та відповідності алгоритмів аналітичних розрахунків вимогам законодавства (розрахунок ПДВ, єдиного податку, єдиного соціального внеску та інших обов'язкових виплат, що можуть впливати на вартість товарів та послуг організації). Саме тому на цьому рівні говорять не про конкретні застосунки, а про програмні системи (1C, ADempiere, Aptean, Bitrix24, IBM, Microsoft Dynamics, Odoo, Oracle E-Business Suite, Salesforce, SAS) або фреймворки, що розробляються, наприклад, в Oracle або Microsoft.

4. Системи прийняття рішень.

Відповідні інформаційні технології з'явилися завдяки зусиллям переважно американських вчених наприкінці 1970-х – початку 1980-х років, що сприяло широкому розповсюдженню персональних комп'ютерів, стандартних пакетів прикладних програм, а також успіху у створенні систем штучного інтелекту. Основною особливістю інформаційних технологій для підтримки прийняття рішень – це якісно новий метод організації взаємодії людини та комп'ютера. Розробка рішення, що є кінцевою метою цієї технології, відбувається в результаті процесу ітерації, в якій беруть участь дві сторони: 1) система підтримки рішень у ролі обчислювальної одиниці та об'єкта управління; 2) людина як керівний елемент, що встановлює вхідні дані та оцінює результат обчислень на комп'ютері. Ітерації відбуваються доки вони не будуть зупинені користувачем

(аналітиком / керівником). Дана технологія дозволяє інформаційній системі разом із користувачем створювати нову інформацію для прийняття рішень.

Інформаційні технології для підтримки рішень можна використовувати на будь-якому рівні управління із функцією узгодження рішень на різних рівнях управління. При цьому дані технології можуть включати в себе функціональні можливості попередніх технологій (обробки та аналізу даних, візуалізації). Головною відмінністю систем такого рівня є наявність не лише розвинутої (ієрархічної) бази даних та бази (математичних) моделей, а й підсистем управління цими базами даних (СУБД) та базами моделей (СУБМ) з системою управління інтерфейсом між користувачем (аналітиком, керівником) і комп'ютером.

Саме в базах моделей передбачено активне використання аналітичної складової, оскільки кожна модель є математичною інтерпретацією проблеми, що за допомогою певних алгоритмів сприяє отриманню корисної для особи, що приймає рішення, інформації. Безпосередньо моделі різняться за метою використання (ті, що оптимізують, та ті, що описують), за засобом оцінки (детерміністичні та стохастичні), за сферою можливого застосування (спеціалізовані та універсальні), за рівнем прогнозування (стратегічні, тактичні, оперативні), окремо виділяється блок математичних моделей як сукупність модельних блоків, модулів, процедур, які дозволяються застосовувати методи лінійного програмування, статистичного аналізу часових рядів, регресійного аналізу тощо.

Якщо інформаційні технології управління передбачають процес самостійного створення візуалізацій (графіків, таблиць), то системи підтримки рішень за замовченням передбачають наявність так званих "dashboard" («приладової панелі») – панелей моніторингу відображення стану процесів, проектів, інших показників діяльності організації, підприємства, установи. При цьому в системі інтерфейсу (GUI) передбачено дві мови – мова користувача та мова повідомлень. Перша використовується відповідно для подання команд на виконання певних дій, чи то у віконно-кнопочному форматі, або командної

строки (скриптів). В свою чергу мова повідомлень – це варіанти формату відповідей системи на запити користувача: текст, аудіо повідомлення, статична (зображення) чи динамічна (відео) графіка тощо.

Системи підтримки рішень мають, в більшості випадків, попит у корпоративних замовників із значною чисельністю персоналу та обсягами фінансових потоків, для яких витрати на подібні застосунки не забаганки, а обов'язковий елемент іміджу організації. На цьому рівні можна повноцінно говорити про корпоративні інформаційні системи. Корпоративна інформаційна система – це набір спеціалізованих програмних та комп'ютерних апаратних засобів або платформ, які створили та налаштовували програмне забезпечення за шкалою комплексу завдань, притаманних сучасним підприємствам. Розробка корпоративних інформаційних систем здійснюється на базі, по-перше, підходів та методів управління підприємствами; по-друге, засобів оптимізації можливостей та продуктивності комп'ютерних систем (Borysenko & Borysenko, 2021).

Взагалі в інформаційних технологіях всі існуючі інформаційні системи, що орієнтовані на аналіз даних, поділяють на дві категорії, що визначаються змістом задач, а саме OLTP- та DSS-системи.

OLTP (on-line transaction processing) система – це системи оперативної обробки транзакцій, що дозволяє одночасно виконувати велику кількість транзакцій (операцій) великої кількості користувачів. Системи OLTP мають регулярний і навіть інтенсивний потік простих транзакцій у вигляді замовлень, платежів, запитів тощо. Дані в системі зберігаються у форматі нормалізованих реляційний таблиць (Azzalini & Scarpa, 2012, p. 6-8).

DSS (decision support system) системи або системи підтримки прийняття рішень виникли хронологічні пізніше за OLTP. Зміст операцій в даних системах полягає в формулюванні більш складних запитів, пов'язаних із аналізом даних, моделюванням процесів предметної області, прогнозування, пошуку взаємозалежності між змінними, реалізації аналітичних дій «якщо то» і тому подібне. Під системою підтримки прийняття рішень слід розуміти людино-

машинний обчислювальний комплекс, орієнтований на аналіз даних, що забезпечує отримання інформації, необхідної для прийняття рішення в сфері управління (Bandyopadhyay, 2023).

DSS-системи поділяються на два типи: статичні та динамічні. Статична система або EIS (Executive Information Systems) система або інформаційна система керівника є сукупністю заздалегідь визначених множин запитів, виконуваних щоденно, які не можуть відповісти на всі питання в разі прийняття рішення (Nord & Nord, 1995).

Повною протилежністю є динамічні DSS-системи, що орієнтуються на обробку нерегламентованих запитів аналітиків до даних на основі концепції OLAP, що стала основою для сучасних концепцій розробки корпоративних інформаційних систем: сховища даних (Data Warehouse), оперативної аналітичної обробки OLAP (On-Line Analytical Processing) та інтелектуального аналізу даних (Data Mining) (Hasan & Hyland, 2001).

Як і з технологіями управління, на рівні систем підтримки рішень краще говорити про компанії, що надають послуги з розробки, впровадження відповідних інформаційних рішень в господарську діяльність, ніж про назви конкретних застосунків. Так, найбільш популярними виробниками корпоративних рішень є: Apache Software Foundation, Clickhouse Inc, IBM, icCube, Jedox, Kyvos Insights, Microsoft, Oracle, Pentaho, SAP, SAS Institute.

Серед одиничних інформаційних систем (програмне забезпечення, що можна встановити на персональному комп’ютері / ноутбуці), які дозволяють здійснювати аналітико-статистичний аналіз даних можна виділити такі: IcCube, GNU PSPP, Microsoft PowerBI, SageMath, Scilab, STATA, Tableau та численні застосунки компаній IBM (Watson, Cognos Analytics, Planning Analytics, SPSS) та SAS (Anti-Money Laundering, Detection and Investigation, Viya Portfolio, Visual Analytics).

Доречи про продукти останніх двох гігантів індустрії аналітико-статистичного програмного забезпечення. Якщо більшість виробників подібних продуктах акцентують увагу на можливостях своїх застосунків виконувати

складні математичні розрахунки, то IBM і SAS активно пропонують свої продукти, що спроможні автоматизувати будь-яку аналітико-статистичну діяльність, а також, в меншій мірі IBM, в більшій мірі SAS, рішення з протидії шахрайству, корупції, відмиванню грошей та іншим зловживанням / правопорушенням на робочому місці.

Одним із головних недоліків цих застосунків є їх пропрієтарність, тобто приналежність до платного програмного забезпечення (вартість ПЗ можливо визначити лише за умови безпосереднього спілкування з відділом продажів, що має спочатку сформувати так зване технічне завдання, що й визначає остаточну вартість програмного забезпечення. Альтернативою даним рішенням слугує FOSS (free and open-source software) – відкрите та безкоштовне програмне забезпечення, точніше, в контексті аналітико-статистичних технологій, мови і програмного середовища для статистичних обчислень, аналізу, візуалізації даних R та Python. Безкоштовність рішень компенсується необхідністю у аналітиків відповідних компетенцій аналізу даних з використанням даних мов, розумінні принципів роботи та розумінні їх переваг та недоліків. Можливості застосунків значно розширюються додатковими пакетами (бібліотеками), серед яких також є пакети, що дозволяються здійснювати будь-який аналітико-статистичний аналіз, в тому числі, алгоритми з пошуку аномалій.

Як було зазначено раніше, окремим напрямом розробки інформаційних системи є інструменти навігації у сховищах даних, необхідність розробки яких пов’язана з необхідністю розробки ефективних технологій пошуку, які дозволяли б ефективно обробляти великі обсяги не тільки «сирих» даних, але сформованих на їх основі аналітики – вітрин даних, графічної інформації, дашбордів (dashboard) тощо. Серед найбільш популярних комерційних корпоративних пошукових систем можна виділити:

– Algolia ("The flexible AI-powered Search & Discovery platform");
– IBM Watson Discovery ("IBM Watson Discovery");
– Yext ("Power Your Website with the World's Best Search");

– Swiftype ("A Powerful Search Experience for Your Website - Without the Learning Curve");

– SearchUnify ("SearchUnify for Sales & Customer Service") і т.п.

Серед корпоративних пошукових систем з відкритим кодом:

– ElasticSearch ("Elastic: Search More, Spend Less");

– Solr ("Solr is the popular, blazing-fast, open source enterprise search platform built on Apache Lucene");

– Sphinx ("Introduction to Search with SPHINX") тощо.

Серед найвідоміших бібліотек, що реалізують технології пошуку, можна назвати:

– Apache Lucene (ElasticSearch, Solr, MongoDB Atlas Search, Datafari, CrateDB) ("Welcome to Apache Lucene");

– Apache Lucy ("The Apache Software Foundation");

– FTS, Tsearch2, RUM, GIN, OpenFTS, GIST (Postgres) (Bartunov, 2018);

– Sphinx/Manticore ("Open-source Database for Search Applications");

– Indri (Lemur) ("INDRI: Language modeling meets inference networks");

– Fulltext (MySQL) ("MySQL: Full-Text Search Functions");

– Terrier ("Welcome to the Terrier IR Platform");

– Manatee ("NLP-Center: NoSketch Engine");

– iSearch Library (ArangoSearch) ("ArangoDB: Powerful Search Included");

– Lunar ("LUNR: Search made simple");

– Xapian ("Xapian: Open Source Search Engine Library").

5. Експертні системи.

Найбільший прогрес серед комп’ютерних інформаційних систем відзначається у галузі розробки експертних систем на основі використання штучного інтелекту. Експертні системи надають можливість керівнику чи аналітику отримувати експертні консультації щодо будь-яких проблем, про які ці системи накопичили знання. В основі експертних систем покладені технології штучного інтелекту. Робота в галузі штучного інтелекту не обмежується експертними системами. Вони також включають створення роботів, систем, які

моделюють нервову систему людини, її слух, зір, запах та здатність вчитися. Застосування експертних систем в якості інструменту попередження / протидії шахрайству чи корупції найбільш доречно до ситуацій, пов'язаних із придбанням / реалізацією товарів та послуг, коли існує значний ризики застосування шахрайських / корупційних схем (Berru, Batista, Torres-Carrión, & Jimenez, 2020).

Технології штучного інтелекту тісно пов'язані із технологіями автоматизації самого процесу отримання інформації, точніше, належного аналізу (добування) даних – data mining, та створення нових знань – knowledge discovery. Поняття "data mining" та "knowledge discovery" були введені у використання в першій половині 1990-х років Усамою Файяд (Usama Fayyad), Григорієм П'яцьким-Шапіро (Gregory I. Piatetsky-Shapiro) та їх колегами, під яким мали на увазі процеси пошуку залежностей у даних, результатом якого є поява нового знання (Cios, Pedrycz, & Swiniarski, 1998).

Data mining – це «процес виявлення в сирих даних раніше невідомих, нетривіальних, практично корисних, доступних інтерпретації знань, необхідних для прийняття рішень у різних сферах людської діяльності» (Azzalini & Scarpa, 2012). Як і з поняттям «штучний інтелект», дослівний переклад з англійської на українську словосполучення "data mining" як «розкопки (або видобуток) даних» також можна вважати невдалим. Knowledge discovery (дослівно – «відкриття знань») – процес отримання нового знання на основі накопичених емпіричних даних (Abellera & Bulusu, 2018, p. 3-4). Тому в україномовному середовищі терміни "data mining" та "knowledge discovery" краще перекладати як «інтелектуальний аналіз даних».

Інтелектуальний аналіз даних передбачає, що:

1) дані можуть бути неточними, неповними, суперечливими, різнорідними, гігантських розмірів, для розуміння яких у конкретних обставинах потребує значних інтелектуальних зусиль;

2) самі алгоритми аналізу даних можуть містити в собі «елементи інтелекту», зокрема, здатність навчатися за прецедентами, тобто можливість

загальні висновки на основі часткових спостережень, розробка яких також потребує значних інтелектуальних зусиль;

3) процеси переробки сирих даних на інформацію, а інформації на знання, що не може відбутися за старою схемою, тому і вимагає нетривіальної автоматизації.

За складом розв'язуваних завдань інтелектуальний аналіз даних практично не відрізняється від стандартного набору інструментів, застосовуваних із середини XX століття в області прикладної статистики, машинного навчання (machine learning), інформаційного пошуку (information retrieval). Основна відмінність полягає в ефективності алгоритмів та технологічності їх застосування.

Найбільшого успіху застосування експертних систем як аналітико-статистичної технології в господарській діяльності зафіксовано в діяльності так званої «Великої четвірки». «Велика четвірка» – найбільша у світі мережа аудиторських та консалтингових компаній: Deloitte, PricewaterhouseCoopers, Ernst & Young та KPMG.

Аналізуючи зміст існуючих експертних систем та систем підтримки рішень, можна прийти до висновку про їх подібність, оскільки обидві системи забезпечують високий рівень підтримки рішень. Однак є три суттєві відмінності. По-перше, вирішення проблеми в рамках систем підтримки рішень відображає рівень її розуміння користувачем (аналітиком / керівником) та його здатністю отримувати та розуміти рішення (Bandyopadhyay, 2023). Технологія експертних систем, навпаки, пропонує такі рішення, що можуть перевищувати інтелектуальні можливості користувача (I. Gupta & Nagpal, 2020). По-друге, відмінність між цими технологіями полягає у здатності експертних систем пояснювати свої міркування в процесі отримання рішення (*Explainable AI: Foundations, Methodologies and Applications*, 2023). Дуже часто ці пояснення більш важливіші для користувача, ніж саме рішення. Нарешті, третя відмінність пов'язана з використанням нового компонента інформаційних технологій – знань. Якщо експертна система розпізнає ситуації, для яких вона не була

призначена (розроблена), вона має повідомити користувача про ненадійність власних відповідей (Kangra & Singh, 2023).

Вважаємо за потрібне ще сказати про машинне навчання та штучний інтелект. Це дві тісно пов'язані, але різні концепції в галузі комп'ютерних наук. У загальному сенсі штучний інтелект – це область науки, яка прагне створити машини, які можуть діяти за допомогою інтелекту, аналогічного людському. Машинне навчання – це одна з технологій, що використовуються для створення таких машин.

В загальному сенсі машинне навчання – це методологія, що дозволяє комп'ютерам навчатися з урахуванням даних без явного програмування. Замість розробки програми, яка вирішує певне завдання, алгоритми машинного навчання використовують для навчання комп'ютера набори даних, виходячи з яких штучний інтелект самостійно створює власну логіку розмірковування (формулювання умовиводів на основі існуючих даних, фактів, прецедентів).

Штучний інтелект, з іншого боку, є більш загальним поняттям, яке охоплює всі технології, спрямовані на створення комп'ютерних систем, які можуть діяти інтелектуально, тобто сприймати, обробляти та використовувати знання та вирішувати завдання, які потребують людського інтелекту. Технології штучного інтелекту можуть використовувати методи машинного навчання, але можуть включати інші підходи, такі як системи експертних знань, вирішення завдань на основі знань і нейронні мережі. Таким чином, машинне навчання є одним із методів, що використовуються в галузі штучного інтелекту. Обидва ці поняття використовуються в різних галузях, включаючи пошук корупції, де машинне навчання може використовуватися для аналізу великих обсягів даних, а штучний інтелект може використовуватися для розробки систем, які можуть приймати рішення на основі цього аналізу.

За твердженнями (Köbis et al., 2021; Odilla, 2023), технології, в основі яких покладено алгоритми, методи штучного інтелекту та/або машинного навчання створили нову категорію застосунків, відмінних від традиційний або класичних методів реалізації аналітико-статистичних процедур. Головною відмінністю

новітніх засобів вважається можливість їх функціонування в автономному режимі, тобто без участі людини.

Як зазначено у більшості робіт (Berk, 2019; P. Gupta & Bagchi, 2024; Korstanje, 2022; Lantz, 2023; Suthaharan, 2016; *Using Machine Learning for Anti-Corruption Risk and Compliance*, 2021), розрізняють три основні парадигми машинного навчання, кожна з яких має свої властивості та сфери застосування. У разі контрольованого навчання (supervised learning) комп'ютер отримує навчальний набір даних, де кожен приклад уже має правильну відповідь, і створює модель, що здатна прогнозувати результати для нових, раніше невідомих прикладів. Це навчання з учителем, яке чудово підходить для завдань класифікації (наприклад, виявлення шахрайських транзакцій чи спам-листів) та регресії (наприклад, прогнозування ціни товару або рівня ризику).

Неконтрольоване навчання (unsupervised learning), навпаки, працює без міток і шукає приховані структури всередині даних. Алгоритми такого типу намагаються кластеризувати або знизити розмірність даних, знаходячи закономірності, які недоступні людському погляду. Це особливо корисно в умовах, коли обсяг даних величезний, але структура невідома, як-от у задачах сегментації клієнтів або аналізу ринку. Ця парадигма відкриває широкі перспективи для соціальних досліджень, адже дозволяє побачити групи чи патерни, які не були задані наперед.

Нарешті, підкріплювальне навчання (reinforcement learning) описує ситуації, коли комп'ютер навчається на основі винагороди чи покарання, поступово вдосконалюючи свої дії в динамічному середовищі. Це навчання зосереджене на поведінці й взаємодії з навколишнім світом – його застосовують у складних завданнях, таких як навчання автономних агентів, робототехніка або стратегічні ігри. Тут комп'ютер діє як експериментатор, що вчиться на власних помилках, наближаючись до оптимальних стратегій.

Якщо говорити про типи завдань, які розв'язує машинне навчання, слід виокремити три ключові категорії: класифікація, регресія та кластеризація. Класифікація передбачає передбачення категоріальних змінних (наприклад,

визначення статі чи класу об’єкта), регресія – прогнозування безперервних величин (наприклад, ціни або температури), а кластеризація – групування даних за схожістю без наперед заданих міток. Ці завдання, хоча й різні за своєю суттю, об’єднані спільною теоретичною базою та потребують якісної підготовки даних, ретельного налаштування моделей і постійного вдосконалення результатів.

У контексті розвитку машинного навчання важливу роль відіграють не лише концепції та алгоритми, а й інструментарій, що забезпечує їхнє практичне впровадження. Серед мов програмування найбільш популярними є Python та R, які завдяки своїй гнучкості, величезній екосистемі бібліотек і відкритому коду стали фактичним стандартом у галузі. Поряд з ними використовуються SAS, Julia, Java, JavaScript і Scala – ці мови забезпечують специфічні переваги залежно від масштабу операцій та вимог до інтеграції з іншими системами.

Особливе значення для машинного навчання мають бази даних, серед яких можна виділити SQL та NoSQL системи, а також Hadoop та Spark, які забезпечують ефективну обробку великих масивів даних. Саме дані формують підґрунтя для навчання моделей, тому можливість їх масштабованого зберігання та швидкої обробки стає критичною умовою для успіху аналітичних проєктів. У поєднанні з інструментами візуалізації, такими як D3.js чи Tableau, ці технології дозволяють не лише аналізувати дані, а й дохідливо представляти результати, що підвищує їхню практичну цінність.

Не менш важливим є використання відкритого програмного забезпечення, серед якого слід відзначити Scikit-learn, Keras, PyTorch, TensorFlow, MXNet, Caffe та Weka. Ці бібліотеки та фреймворки пропонують готові модулі для побудови, тренування та тестування моделей машинного навчання, що значно скорочує час розробки й дає змогу зосередитися на постановці завдань і налаштуванні алгоритмів.

У сучасних дослідженнях машинного навчання та аналітики даних значну роль відіграють спеціалізовані платформи, що об’єднують інструменти для розробки, тренування, тестування й розгортання моделей. Для подібних платформ використовується абревіатура DSML (data science and machine

learning). Згідно з (Jaffri et al., 2024), платформи DSML – це інтегровані програмні рішення, що пропонують набір базових компонентів для створення аналітичних рішень і впровадження їх у бізнес-процеси. Вони підтримують повний цикл роботи з даними – від збору й підготовки до моделювання, розгортання та моніторингу, забезпечуючи одночасно доступ як для технічних команд, так і для бізнес-користувачів. Сучасні DSML-платформи дедалі частіше поєднують традиційні моделі машинного навчання з генеративним ШІ (GenAI), що відкриває нові горизонти для автоматизації, оптимізації процесів і прийняття управлінських рішень.

На ринку спостерігається висока конкуренція, серед яких лідерами є Microsoft, Google, Amazon, Dataiku, DataRobot, SAS та Databricks. До категорії інноваційних платформ (visionaries) належать H2O.ai, Cloudera та Domino Data Lab, представники вузької ніші – KNIME, Anaconda, Altair, MathWorks, Posit та Alteryx. Дві платформи (IBM і Alibaba Cloud) представляють категорію амбітних гравців, що не мають явних переваг, однак спроможні на суттєві результати. Кожен із цих постачальників має свою стратегію: деякі зосереджуються на демократизації аналітики для бізнесу, інші – на забезпеченні складних сценаріїв використання для експертних команд, ще інші – на розвитку генеративних моделей чи інтеграції з гібридними інфраструктурами.

Отже, на сьогодні існує безліч платформ для машинного навчання, кожна з яких має свої переваги, обмеження й спеціалізацію. Вибір оптимальної платформи залежить від завдань, що ставить перед собою організація, технологічного стеку, яким вона вже володіє, а також фінансових і технічних ресурсів. В умовах дедалі жорсткішої конкуренції між постачальниками сервісів штучного інтелекту, жодна компанія не може дозволити собі зупинитися, адже кожне нове рішення швидко копіюється конкурентами. У межах нашої дисертації важливо розуміти, що вибір платформи – це не лише питання технологій, а й стратегічного бачення, яке визначає, як саме аналітичні інструменти будуть інтегровані в практику попередження / протидії корупції та управлінських інновацій.

6. Генеративний штучний інтелект.

Починаючи з 2023 року більшість існуючих на ринку інформаційних продуктів інтегрує сервіси штучного інтелекту, точніше генеративного штучного інтелекту. Генеративний штучний інтелект (Generative AI, GenAI) – це напрям розвитку штучного інтелекту, що виходить за межі звичайного аналізу або класифікації даних. Його суть полягає не лише у здатності розпізнавати закономірності в наданих прикладах, а й у тому, щоб на основі цих закономірностей створювати принципово нові дані, яких ніколи не було в навчальних наборах. Це означає, що якщо традиційний ШІ допомагає нам передбачити, до якої категорії належить об'єкт або яке наступне слово в послідовності, то GenAI іде далі – він творить, моделює нові варіанти, генерує зміст, який є водночас оригінальним і стилістично або структурно подібним до наданих йому прикладів. Завдяки цій властивості, генеративний ШІ знайшов застосування у найрізноманітніших сферах: від створення реалістичних зображень чи анімацій до написання художніх текстів, генерування музики, побудови віртуальних світів і навіть проектування нових хімічних сполук для медицини .

Найважливішим у розумінні GenAI є те, що він працює не на рівні запам'ятовування готових рішень, а на рівні ймовірнісних розподілів: модель вчиться на величезних обсягах даних, будуючи уявлення про те, як виглядають «правдоподібні» зразки з цієї множини. Коли ми, наприклад, даємо мовній моделі завдання написати нову історію, вона не просто повторює речення з книг, які читала під час навчання, а створює новий текст, комбінуючи стилістичні та семантичні шаблони, закладені в її ваги та параметри. Технологічно за цим стоять складні архітектури, зокрема трансформери, генеративно-змагальні мережі (GAN), варіаційні автокодери (VAE), кожна з яких дозволяє працювати з різними видами даних – текстом, зображеннями, музикою, відео чи навіть біологічними структурами. Саме тому GenAI можна вважати одним з найбільш універсальних і перспективних інструментів сучасної штучної інтелектуальної революції.

Серед основних постачальників генеративного ШІ сьогодні виділяються кілька компаній, кожна з яких займає свою нішу та пропонує унікальні продукти. OpenAI ("OpenAI platform") є одним із найбільш впливових гравців на ринку завдяки моделям GPT-3, GPT-4, ChatGPT, а також візуальному генератору DALL-E й кодогенератору Codex. OpenAI тісно співпрацює з Microsoft, що дозволяє інтегрувати свої сервіси в хмарну інфраструктуру Azure та використовувати їх у широкому спектрі комерційних і дослідницьких застосувань. DeepMind (підрозділ Google) ("DeepMind : Build AI responsibly to benefit humanity,") також створює відповідні сервіси, наприклад моделі Gopher, AlphaFold, AlphaGo Zero та AlphaZero. Крім того, DeepMind розробила універсальний алгоритм Player of Games (PoG), що показує позитивні результати як у іграх із повною, так і неповною інформацією.

Серед інших важливих гравців варто згадати Cohere ("Cohere : The all-in-one platform for private and secure AI"), яка спеціалізується на моделях для текстового аналізу; Hugging Face, що є найбільшою платформою для відкритих моделей NLP (у тому числі завдяки бібліотеці Transformers і Model Hub) ("Huggingface : The AI community building the future"); AI21 з моделлю Jurassic-1, яка забезпечує API-доступ до великих мовних моделей ("AI21 : Building the Future of Enterprise AI"); InflectionAI, яка розвиває напрям інтуїтивної взаємодії людини з комп’ютером ("Inflection AI : Own your edge"); а також Anthropic ("Antropic : AI research and products that put safety at the frontier"), творця Claude 2 – потужного конкурента ChatGPT, здатного обробляти значно більші обсяги тексту й надавати чистіші відповіді. Кожен із цих постачальників формує унікальний сегмент ринку генеративного ШІ, просуваючи власні технології, сервіси та API, що дозволяють бізнесам, дослідникам і розробникам створювати нові, інноваційні продукти на основі штучного інтелекту.

Отже, аналітико-статистичні системи попередження / протидії корупції є надзвичайно багатовимірними як за функціональними напрямами, так і за технологічними платформами, на яких вони реалізуються. Від класичних інформаційних технологій обробки даних, що автоматизують рутинні процеси

збору й обробки інформації, до складних систем підтримки прийняття рішень – кожен рівень цифрових рішень виконує власну роль у зміцненні прозорості й підзвітності управлінських процесів. Важливість автоматизації даних стає особливо очевидною, коли мова йде про мінімізацію людського впливу на процеси аудиту, що прямо знижує ризики умисних фальсифікацій чи помилок. Саме тому на першому етапі впровадження систем увага концентрується на інтеграції базових, але необхідних інструментів, здатних забезпечити сталість та законодавчу відповідність збору й зберігання даних.

Водночас автоматизація комунікаційних процесів стає не просто технологічною зручністю, а стратегічним інструментом, без якого сучасна боротьба з корупцією є неповною. Системи віддаленої комунікації, що під час пандемії COVID-19 стали новим стандартом для офісної роботи, сьогодні активно застосовуються у контексті опитування свідків, аналізу інформації від підозрюваних та координації антикорупційних підрозділів. Окремо слід зазначити, що автоматизація управління, зокрема за допомогою ERP, CRM та SCM систем, виводить аналітико-статистичні технології на рівень стратегічного впливу: тут мова йде вже не лише про фіксацію подій, а й про їхнє передбачення, аналіз відхилень та моделювання сценаріїв для запобігання корупційним ризикам. Статистичний і візуальний інструментарій, залучений у цих системах, посилює управлінські можливості, роблячи дані не лише джерелом інформації, а й засобом для формування рішень.

Особливо цікавою є поява систем підтримки прийняття рішень, що поєднують людину й машину в інтерактивному процесі аналізу: вони не просто пропонують готові результати, а дозволяють керівникам створювати нові знання, використовуючи симуляції, прогнозування й моделювання. Розвинені підсистеми управління базами моделей і даних, приладові панелі (dashboard) та гнучкі інтерфейси стають стандартом для корпоративних систем, забезпечуючи одночасно високу гнучкість та масштабованість. При цьому окремої уваги заслуговують DSS-системи, які завдяки своїй динамічній природі дозволяють

аналітикам працювати з нерегламентованими запитами, адаптуючи аналіз під конкретні завдання та виявляючи приховані патерни й аномалії.

Нарешті, наше дослідження демонструє, наскільки кардинально змінюють правила гри системи, засновані на штучному інтелекті та машинному навчанні. AI- та ML-підходи відкривають можливості для аналізу величезних обсягів даних, побудови складних прогнозних моделей, а також автоматизованого пошуку аномалій та ризикових сценаріїв. Еволюція аналітики від класичних статистичних методів до інтеграції генеративного ШІ свідчить про стрімкий розвиток індустрії: тепер системи не лише аналізують, а й створюють нові дані, надаючи можливість будувати симуляції, генерувати гіпотези та тестувати їх практично в реальному часі.

3.2. Особливості впровадження інноваційних аналітико-статистичних технологій попередження корупції в державі

Процес впровадження інноваційних аналітико-статистичних технологій як інструменту попередження / протидії корупції в державі може відбувати за двома напрямками – зверху вниз та знизу вверх (Köbis et al., 2021; Köbis, Starke, & Rahwan, 2022). Перший напрям (зверху вниз) базується на тому, що інституції формуються законами, які розробляють політичні лідери (Easterly, 2008). Боротьба з корупцією зверху вниз спрямована на зміну чи регуляцію процесів в державному управлінні за допомогою законотворчої діяльності. Штучний інтелект в цьому плані може бути використаний для підтримки цієї діяльності. Прикладом в цьому може стати проект Kalsada на Філіппінах, що використовує машинне навчання для візуалізації просторових даних, пов’язаних із будівництвом, ремонтом шляхів та оцінювання їх якості для виявлення можливих випадків розкрадання будівельних матеріалів доріг (Kaiser, Rahemtulla, & Van den Brink, 2016). Тут штучний інтелект спроможний значно покращити ефективність порівняно з ручними підходами, які вимагали буквально розкопувати дорогу для оцінки якості використовуваних матеріалів (Olken, 2007). Технології цього напряму стають невід’ємними інструментами в

роботі тих, хто відповідає за боротьбу з корупцією – прокурорів та служб внутрішнього контролю.

Згідно з другим напрямком (знизу вверх), соціальні інститути виникають спонтанно завдяки соціальним нормам, звичаям, традиціям, віруванням та цінностям, що існують в суспільстві (Easterly, 2008). Змістом антикорупційних зусиль є аналіз культурного та соціального контексту з метою виявлення та підтримки існуючих у суспільстві зусиль щодо зменшення рівня корупційних практик (M. H. Khan, Andreoni, & Roy, 2016). Цей підхід в основному спирається на активні організації громадянського суспільства та журналістів, що можуть виконувати функцію моніторингу (Starke, Naab, & Scherer, 2016). Наприклад, український портал Dozorro дозволяє здійснювати аналітико-статистичний аналіз даних порталу державних закупівель Prozorro з метою виявлення корупційних схем (Oksha, 2019).

Обидва напрямки використання штучного інтелекту для боротьби з корупцією відрізняються від технологічних рішень використання штучного інтелекту у боротьбі проти інших форм злочинності, а саме відрізняється тим, що застосунки можуть використовуватися як по відношенню до громадян, так і у зворотному напрямку – перевірки та контролю представників держави.

Таким чином, у межах двох загальних напрямів впровадження інноваційних аналітико-статистичних технологій – як через інституційні, законодавчо-нормативні механізми, так і через ініціативи громадянського суспільства та медіа – формується широкий спектр практичних застосувань. З огляду на це доцільним є зосередження уваги на аналізі сучасних практик упровадження таких технологій, представлених у наукових публікаціях, емпіричних дослідженнях, аналітичних кейсах та експериментальних розробках.

Всю сукупність наявних тематичних публікацій можна поділити за такими напрямками:

1. Аналіз вторинних даних – коли автори намагаються розробити власні індикатори рівня корупції або описати стан розвитку корупційних відносин у певний період часу на основі наявних показників чи відповідних ним досліджень

(Heritage Foundation, Transparency International, ООН, Міжнародний банк тощо) (Adam & Fazekas, 2018; Berru et al., 2020; Davenport & Mittal, 2023; de Francesco & Trein, 2020; Lima & Delen, 2020; Mansour, Taha, & Taha, 2023; Norris, 2020; Odilla, 2023; Zemankova, 2019);

2. Автоматизовані системи аналізу текстових даних – відображають результати впровадження технологій обробки природної мови (аналіз документальних даних, що містять інформацію про корупційні (шахрайські) дії та правопорушення) у поєднанні з технологіями візуалізації просторових даних (Gawthorpe, 2018; López-Iturriaga & Sanz, 2017; Mamun, Azad, & Pramanik, 2023; Noerlina et al., 2018).

3. Методологічний напрям або інструментальні дослідження – у якому дослідники розробляють універсальні методи (алгоритми) аналізу даних (виявлення аномалій) із визначенням можливих сфер їх практичного застосування або розробляють інструменти для автоматизації розумової діяльності, пов’язаної із антикорупційною діяльністю (Aggarwal, 2017; Chatera, Borgib, Slamaa, Sfar-Gandouraa, & Landoulsi, 2022; J. Chen et al., 2023; Dou et al., 2020; Eswar, Kannan, Vuduc, & Park, 2021; Han et al., 2022; Hojjati, Ho, & Armanfard, 2022; Isson, 2018; Kaplan, 2023; Lawless, 2022; Levin, Pomares, & Alvarez, 2016; C. Liu et al., 2022; Lu et al., 2022; Ma et al., 2022; Pang, Shen, Cao, & Hengel, 2021; Pinheiro & McNeill, 2014; Ringsholm, 2022b; Rozenas, 2016; Salehi et al., 2022; Sehwag, Chiang, & Mittal, 2021; Shao et al., 2022; Vaughan, 2020; Vincent et al., 2021; Yatsyna & Kudinov, 2025; Zhao, Chen, & Jia, 2022; Zhao et al., 2021; Zhao, Nasrullah, & Li, 2019; Кудінов & Яцина, 2024).

4. Експериментальні розробки – результати практичного впровадження технологій машинного навчання та штучного інтелекту для ідентифікації суб’єктів корупційних відносин та/або отримання статистично обґрунтованого підтвердження наявності чи відсутності корупції (Alvarez, Levin, & Li, 2018; Chan, Hogaboam, & Cao, 2022; Hassan, Passing, & Goméz, 2023; Hicken & Mebane, 2017; Klimek, Jimenez, Hidalgo, Hinteregger, & Thurner, 2018; Klimek, Yegorov, Hanel, & Thurner, 2012; Kobak, Shpilkin, & Pshenichnikov, 2016, 2020; Kudinov &

Yatsyna, 2025; Lacasa & Fernandez-Gracia, 2019; X. Li et al., 2020; *Machine Learning Applications for Accounting Disclosure and Fraud Detection*, 2021; Mebane, 2015; Mebane & Klaver, 2015; Mebane & Wall, 2015; *Next-generation AML: 6 Tips to Modernize Your Fight Against Money Laundering*, 2023; Ringsholm, 2022a; Rozenas, 2017; Steif, 2022; *Using Machine Learning for Anti-Corruption Risk and Compliance*, 2021; Zhang, Alvarez, & Levin, 2019).

Розглянемо далі найбільш цікавіші моменти.

1. Аналіз вторинних даних.

Дослідження (Lima & Delen, 2020) презентує результати використання методів машинного навчання для виявлення фактів корупції на основі розширених нелінійних моделей з високим рівнем точності прогнозування. Автори підсумували, що відкритість уряду (90,47%), захист прав власності (78,84%), належно функціонуюча судова система (77,94%), а також високий індекс освіти (53,93%) є найбільш впливовими факторами визначення рівня корупції. Ці висновки були зроблені на основі 30 моделей, реалізованих з використанням набору показників 132 країн за 2017-2018 роки: індексу простоти ведення бізнесу, даних фондів Heritage Foundation, Transparency International, а також звітів про розвиток людського капіталу ООН (див. рисунок 3.1).

Як зазначили дослідники, найбільшу ефективність показав метод Random Forest (точність 85,77%). Метод опорного вектору (SVM) та метод нейронних мереж (artificial neural networks) показали меншу точність (76,15% та 73,84% відповідно). Для виконання запропонованої методології було використано ряд програмних засобів, зокрема Microsoft Excel, Tableau, SAS JMP і KNIME.

У статті (Berru et al., 2020) про дослідження корупції в державних закупівлях було використано метод систематичного огляду літератури Торрес-Каррион. Вчені обрали 102 наукові статті, опубліковані в базах WOS та SCOPUS за 2015-2019 роки, присвячені дослідженню корупції, та здійснили аналіз із застосуванням технології штучного інтелекту. Аналіз вибраних статей дозволив авторам відповісти на наступні 4 питання:

– про методи, що використовуються для дослідження корупції в сфері державних закупівель (What methods are being applied to investigate corruption in public procurement contracts?);

– про характеристики організацій щодо яких проводяться розслідування (What are the characteristics of the organizations in which the research has been carried out?);

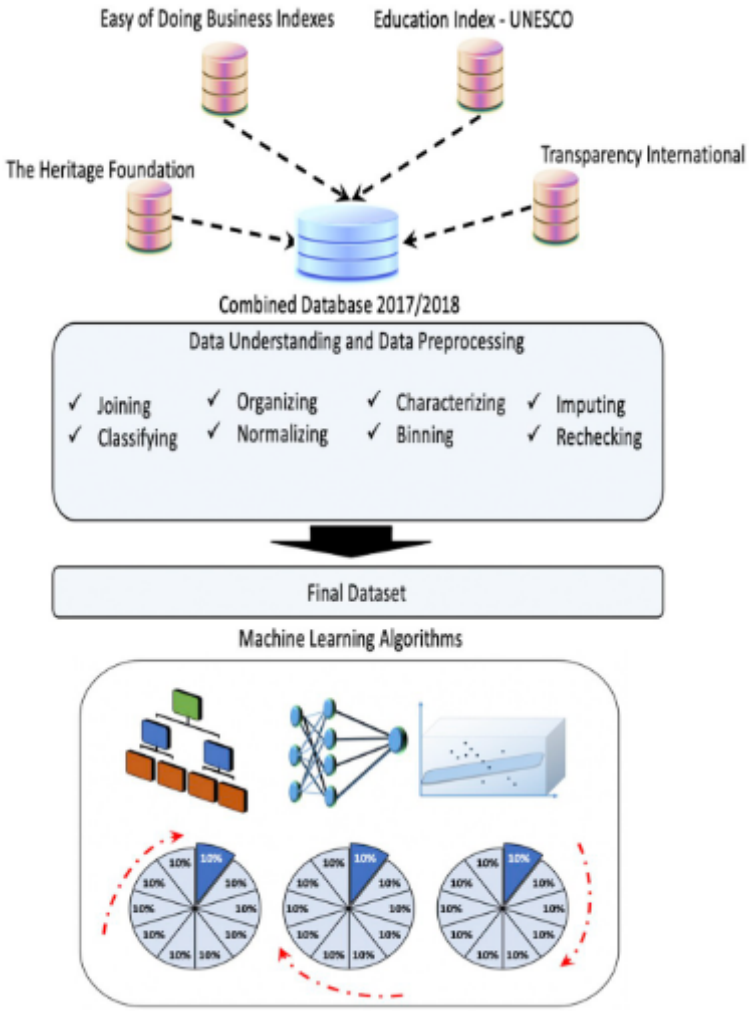

Рис. 3.1 – Графічне зображення методологічного підходу кросвалідації, яка використовується для тренування і тестування 30 моделей (10 різних моделей для кожного типу алгоритму) (Lima & Delen, 2020, p. 10)

– про технологічні інструменти, що використовуються для дослідження виявлення та запобігання корупції в системі державних закупівель (What technological tools are being used to investigate the detection and prevention of corruption?);

– про алгоритми, методології та інструменти аналізу даних, що використовуються для виявлення корупції в системі державних контрактів (What algorithms, methodologies, and data analysis tools are used to detect corruption?).

В рамках нашого дослідження цікавими є 1, 3 та 4 питання. Як виявилося, 87% дослідників працюють із структурованими базами даних, оскільки за методологією дослідження переважають кількісні дослідження (88%). Найбільш часто використовуваний метод – кореляційний аналіз (77%). При цьому 68% досліджень розроблено саме в сфері (field of science) інформаційних технологій. Інші дослідження стосуються таких наукових напрямків як економіка, математика і статистика. Політологія і соціологія у переліку не представлені. Половина (50%) досліджень сфокусовано на сфері бізнесу, 31% досліджують публічну (державну) сферу. У 89% досліджуваних статей автори використовують застосунки для персональних комп'ютерів (desktop).

Більшість дослідників (92%) використовувало для аналізу масиви структурованих даних (бази даних) з метою виявлення (descriptive) фактів корупції (79%), решта розробляли прогнозні моделі з метою попередження корупції. Серед конкретних методів аналізу найбільш застосовуваними виявились методи лінійної регресії (16%) та Байєсовські методи (16%). У меншій мірі застосовуються теорія множин, теорія графів, обробки природної мови, метод k-середніх. Серед методів отримання нового знання переважали методи класифікації (54%) та кластеризації (43%). Найпоширеніші технологічні середовища (technological tools) для аналітико-статистичних досліджень – Python Java, Matlab, Weka. Менш згадувані такі назви як R, RapidMiner, Hadoop, Spark, Neo4j, Casandra, Kafta, Visual Studio.

2. Автоматизовані системи аналізу текстових даних.

У статті (López-Iturriaga & Sanz, 2017) проаналізовано рівень корупції в 52 провінціях Іспанії, які, незважаючи на єдність держави, наділені досить високим ступенем політичної та економічної автономії. Автори дослідження, використовуючи матеріали іспанської щоденної газети El Mundo, створили масив даних про кримінальні справи, пов'язані із корупційними злочинами, в

яких фігурували державні службовці за період з 2000 по 2017 роки, і навчали штучну нейронну мережу “SOMs” (self-organizing maps – самоорганізаційні карти) аналізувати подібні публікацій та визначати рівні корумпованості регіонів за допомогою розрахунку відповідного показника (на 100 тисяч жителів) (див. рисунок 3.2). Під час аналізу перевірялася гіпотеза про вплив на рівень корупції оподаткування нерухомого майна (real estate taxation), державного боргу на душу населення в регіоні (debt per capita), загально боргу за послуги (debt service), економічного зростання (deposit institution growth), чисельності населення (population growth), динаміки зареєстрованих компаній (variation in the number of registered companies), цін на житло (house price increase), рівня безробіття (unemployment rate та unemployment rate growth), підтримки правлячої партії (governments ruling in majority) та періоду перебування правлячої партії при владі (number of years in government). В результаті дослідження гіпотеза про різницю між корупційними та некорупційними регіонами країни, що спричинені кореляцією корупції із обсягом інвестицій, цінами на нерухомість, кількості депозитних установ, а також тривалістю періоду перебування при владі певної партії, була підтверджена. У той же час, наявність державного боргу та кількість голосів правлячої партії не були пов'язані з рівнем корупції в регіоні.

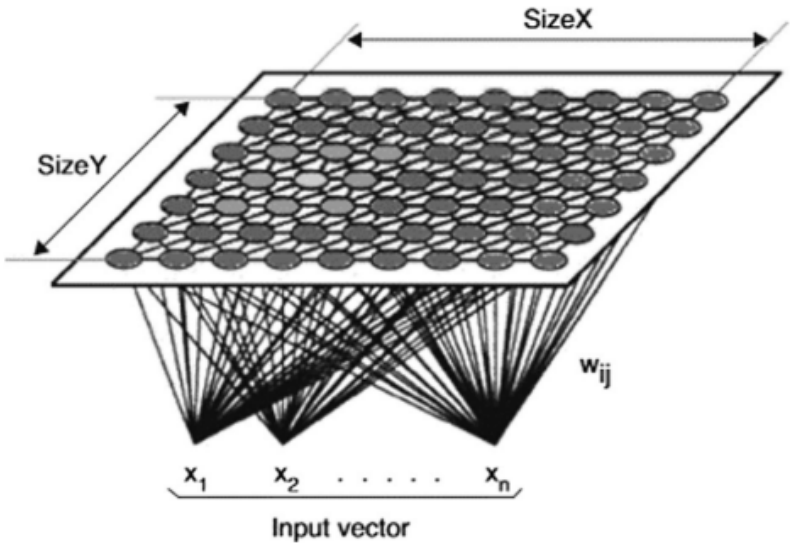

Рис. 3.2 – Графічна репрезентація системи SOM
(López-Iturriaga & Sanz, 2017, p. 980)

Однією з переваг роботи є розроблена модель підвищення ефективності заходів антикорупційної боротьби. В умовах обмежених ресурсів органи влади можуть використовувати систему раннього попередження про корупцію, яка класифікує кожний регіон країни відповідно до її профілю корупції, що дозволяє здійснювати відповідну профілактичну або «адресну» політику попередження / протидії корупції. Також модель дозволяє прогнозувати корупційні випадки задовго до їх виявлення, що посилює першочергові заходи.

Наступне дослідження (Noerlina et al., 2018) представило веб-застосунок із функцією збору інформації з новинних сайтів провінцій Індонезії, уточненням, класифікацією змісту залежно від кількості та ступеня корупційних правопорушень та візуалізації результатів на географічній мапі (див. рисунок 3.3).

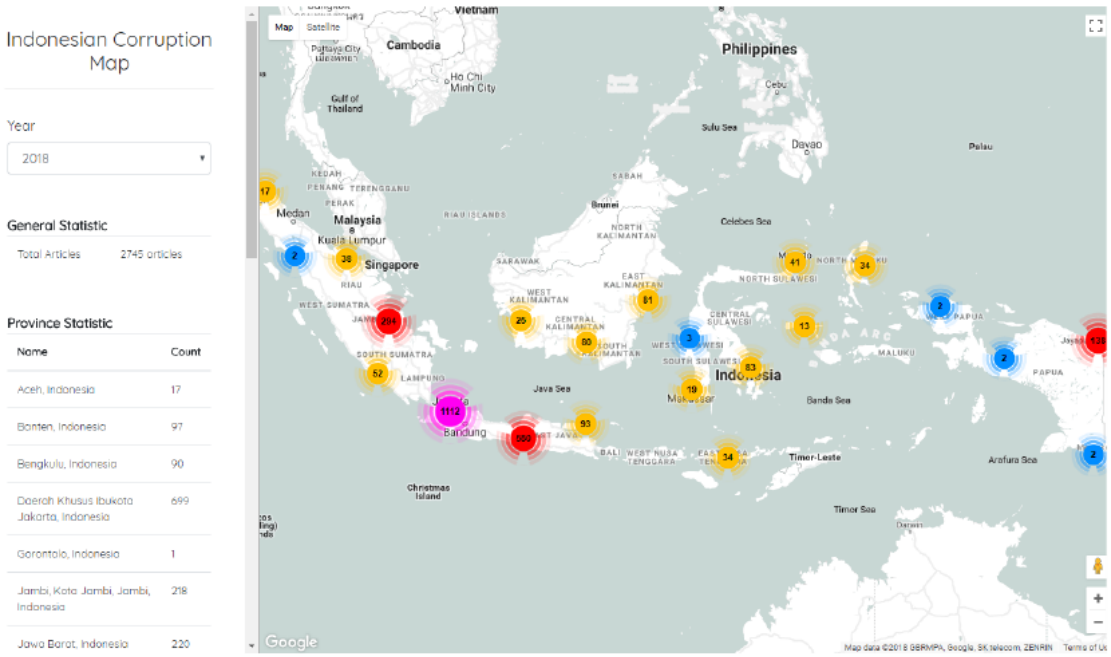

Рис. 3.3 – Графічний інтерфейс для застосунку Indonesian Corruption Map (Noerlina et al., 2018, p. 404)

Веб-застосунок було розроблено з використанням фреймворку Laravel та Google Maps API. Під час дослідження була зібрана інформація з 7 новинних сайтів Індонезії (liputan6.com, tribunnews.com, merdeka.com, kompas.com, detik.com та tampo.co) за останні останніх 7 років (2010–2017). З 900 000 статей

новин близько 2 000 статей (0,2%) відносилося до категорії статей про корупцію. Рівень корупції на мапі визначався за допомогою кольору: від синього (незначні випадки корупції) до яскраво-рожевого (значні випадки корупції).

Для візуалізації збільшення або зменшення кількості випадків для кожної провінції наявна можливість розкрити хронологічну схему, яка показує щомісячну або щорічну динаміку корупційних правопорушень. В цілому, за допомогою карти корупції, за свідченнями авторів публікації, можна чітко і детально відобразити візуальну мапу корупції в Індонезії з урахуванням географічного розташування провінції та хронологічної ретроспективи Це дозволяє більш об'єктивно приймати державні рішення та розробляти ефективні програми зменшення корупції.

Аналогічну методологію було використано в роботі (Hlatshwayo et al., 2018), що представила концепцію міждержавного індексу новин про корупцію (NIC) та індексу новин про боротьбу з корупцією (anti-NIC), з подальшою оцінкою впливу цих індексів (див. рисунок 3.4).

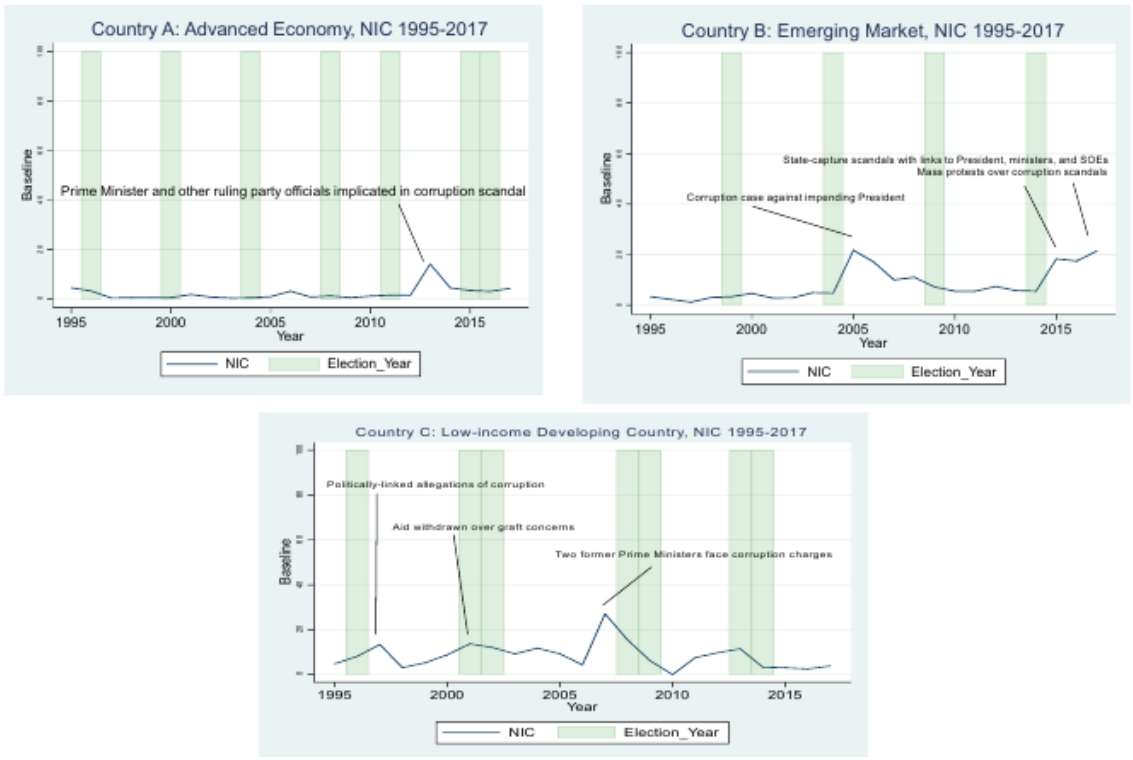

Рис. 3.4 – Приклад розрахунку індексу NIC для трьох країн (Hlatshwayo et al., 2018, p. 15)

Назва індексу найбільше відображає його вміст – це карта новин про корупцію, а не про саму корупцію, оскільки не завжди інформація про корупцію потрапляє до новинних сайтів. Перевагою підходу, на думку авторів, є можливість відстежувати частоту змін у країнах за порівняний період, здатність охоплювати корупційні скандали, а також відсутність потреби покладатися на суб'єктивні та часто дуже ангажовані думки місцевих експертів. Однак суб'єктивність при виборі інформації для публікації на сайті та надійність опублікованої інформації не дозволяє говорити про щось більше, ніж про новини про корупційні правопорушення.

Висновки дослідження підтверджують вплив новин на корупційні акти та антикорупційні заходи, особливо в країнах перехідної економіки. В результаті дослідження було підтверджено гіпотезу про стабільний негативний вплив NIC на економічне зростання в тривалому періоді. Крім того, автори роблять висновок, що для успішних антикорупційних зусиль недостатньо використовувати лише індекс anti-NIC, проте зафіксовано позитивний вплив індексу anti-NIC на індекс NIC. Інформація про використані інформаційні технології в першоджерелі відсутня.

3. Методологічний напрям (інструментальні дослідження).

Дана категорія робіт суттєво відрізняється від попередніх категорій декількома параметрами.

По-перше, метою подібних публікацій є представлення власної інформаційної системи штучного інтелекту чи методу машинного навчання під час вирішення задач пошуку аномалій. Тому, ймовірно, навмисно, для збільшення аудиторії потенційних читачів, автори намагаються охопити максимальну чисельність зацікавлених осіб і декларують, що розроблені та представлені у роботі методи, алгоритми чи технології мають широке використання, починаючи від біології і закінчуючи сферою боротьби з шахрайством (вважай, корупцією).

По-друге, на відміну від публікацій попередніх категорій, роботи в даній категорії представлені у двох форматах: 1) як наукова (в більшості випадків у

вигляді тексту статті, тез за результатами конференції) публікація; 2) як набір застосунків (кодів, скриптів тощо) у профільних соціальних мережах (наприклад, github або kaggle), що дозволяє об'єднувати зусилля різних фахівців, в тому числі, спілкуватися, коментувати, редагувати застосунки один одного з функцією слідкування за версіями коду, а також можливістю відтворювати запропоновані методи самостійно з використанням навчальних чи власних наборів даних.

В цьому плані нам достатньо буде зробити огляд репозиторію на www.github.com. Серед існуючих на ньому проєктів можна виокремити такі:

1. ADBench (Han et al., 2022). ADBentch є спільним проектом дослідників Шанхайського університету фінансів та економіки (SUFE) і Університету Карнегі-Меллона (CMU). Проект розроблено авторами найбільш популярних бібліотек виявлення аномалій, включаючи виявлення аномалій для табличних даних чи баз даних (PyOD), часових рядів (TODS) та графів (PyGOD). За результатами проекту було проведена оцінка продуктивності 30 алгоритмів виявлення аномалій в масивах даних з використанням 57 наборів даних в кількості 98 436 експериментів за трьома параметрами:

– типу методу машинного навчання (supervision): тести працездатності алгоритмів включають 14 алгоритмів контрольованого, 7 напівконтрольованого і 9 неконтрольованого навчання;

– характеру аномалії, що досліджується: локальні, глобальні, кластерні, залежні;

– стійкості і стабільності алгоритму в умовах наявності інформаційного шуму чи неповних даних.

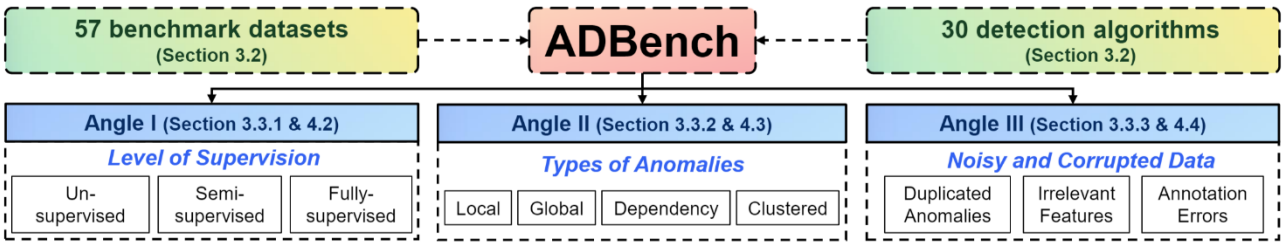

Рис. 3.5 – Загальна характеристика проекту ADBench (Han et al., 2022)

Проєкт поєднав в собі розробки за трьома напрямами – виявлення аномалій в табличних даних, часових рядах та графових даних:

1.1.PyOD представляє собою бібліотеку Python для виявлення аномальних об’єктів у багатовимірних даних. Оригінальний PyOD включає понад 40 алгоритмів виявлення, починаючи від класичного LOF до найсвіжішого ECOD ("Python Outlier Detection (PyOD)," 2023; Zhao et al., 2019).

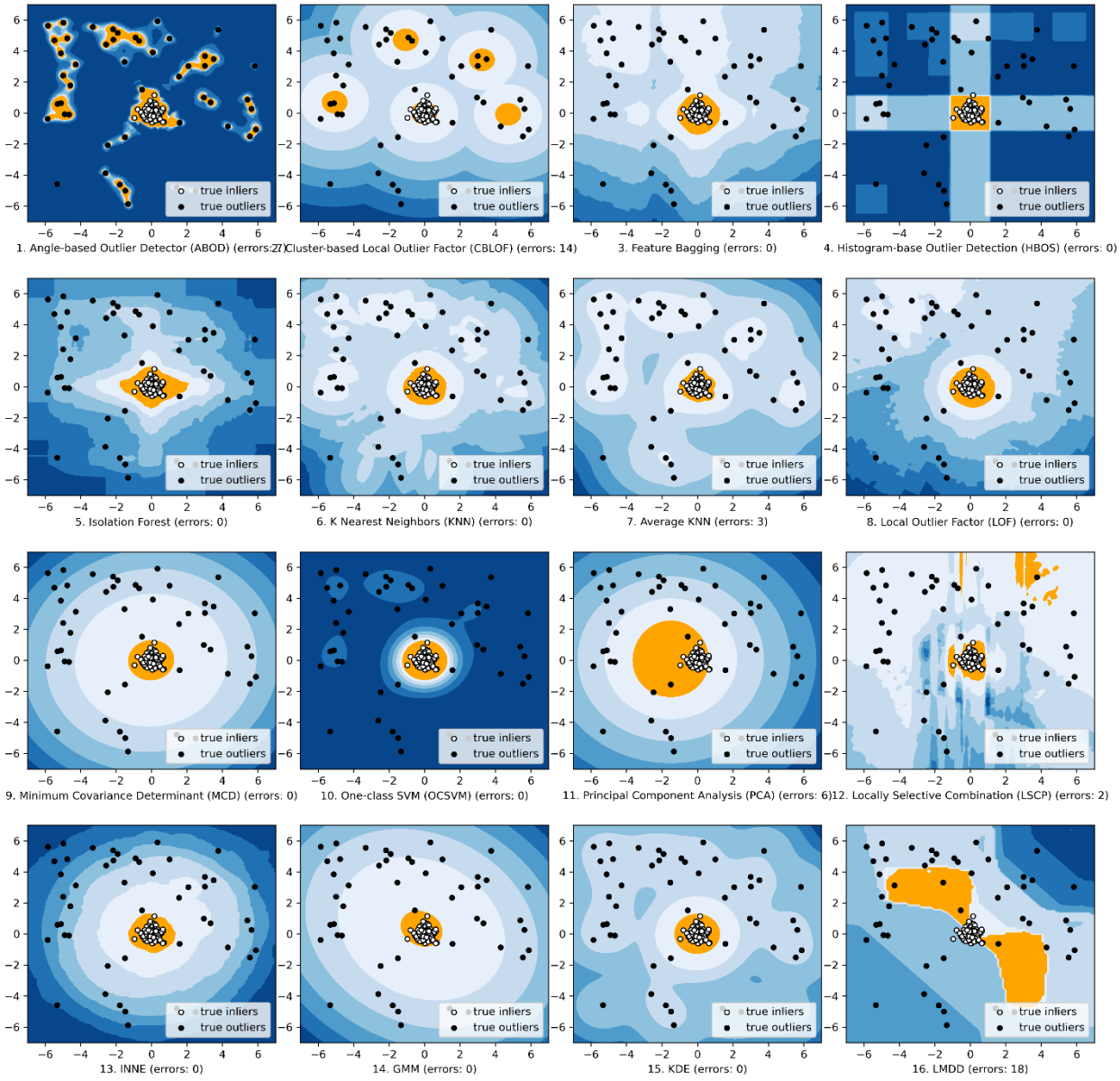

Рис. 3.6 – Приклади візуалізації результатів пошуку аномалій різними алгоритмами ("Python Outlier Detection (PyOD)," 2023; Zhao et al., 2019)

1.2.TODS – це універсальна система автоматичного машинного навчання для виявлення викидів (аномалій) в даних багатовимірних часових рядів. TODS

включає модулі для побудови систем виявлення аномалій на основі машинного навчання, включаючи: обробку даних, обробку часових рядів, аналіз ознак (добування), алгоритми виявлення і модуль посилення. Функціональні можливості, надані через ці модулі, включають попередню обробку даних для загальних цілей, згладжування/ перетворення даних часових рядів, витягування ознак з часових/частотних блоків даних, різні алгоритми виявлення, включаючи алгоритми залучення експертів (людського досвіду) для калібрування системи (Lai et al., 2021; "TODS: Automated Time-series Outlier Detection System," 2023).

1.3.PyGOD – бібліотека Python для виявлення викидів (аномалій) в графах. PyGOD включає в себе понад 10 алгоритмів виявлення аномалій в графах, таких як DOMINANT або GUIDE (K. Liu et al., 2022; "PyGOD," 2023). Однією з переваг даного комплексу алгоритмів є простота їх застосування в сенсі обсягу використання коду – для запуску більшості алгоритмів достатньо 5 строчок коду.

2. Інструментальною можна вважати роботу автора дисертації, пов’язану із автоматизацією розумової діяльності спеціалістів з антикорупційної діяльності, а саме фахівців з управління ризиками, корпортавного управління і комплаєнсу та фахівців з моніторингу та оцінки соціальних проєктів (Kudinov & Yatsyna, 2025; Yatsyna & Kudinov, 2025). Результати роботи пройшли апробацію під час організації виробничих практик для студентів спеціальностей «Політологія», «Соціологія», «Соціологія медіації та кримінології», «Соціальна робота» Факультету соціології та управління Запорізького національного університету (Кудінов & Яцина, 2024).

Вихідний код кожного розробленого застосунку можна знайти на репозиторії GitHub (https://github.com/iitiro) або у додатку А. Для зручності користувачів створено відео-інструкції, які детально пояснюють логіку роботи кожного з них. Серед розроблених застосунків для підтримки антикорупційної діяльності, можна виокремити такі:

2.1.SEARCH_PDF – Python-скрипт, що автоматизує пошук і завантаження PDF-документів за визначеними користувачем ключовими словами. Він є ефективним засобом для збору архівних матеріалів, наукових публікацій, звітів

або офіційних документів, які мають значення для аналізу політичних чи соціальних процесів, в тому числі пов’язаних із проблемами корупції (див. Додаток А.1).

2.2.SEARCH_SCHOLAR – застосунок, що спеціалізується на пошуку публікацій в мережі Google Scholar за заданим списком ключових слів. Інструмент орієнтовано безпосередньо на академічні джерела. Застосунок включає модуль для автоматизації перегляду посилань, завантаження яких не відбулось (у зв’язку з необхідністю мати підписку на академічне джерело або необхідності виконати додаткові дії («клікнути» на відповідну кнопку)) (див. Додаток А.2).

2.3.SEARCH_YOUTUBE – скрипт, який автоматизує пошук відеоматеріалів на платформі YouTube за ключовими словами. Інструмент є цінним для дослідників, що аналізують виступи політичних діячів, дебати, репортажі ЗМІ, або інші візуальні дані, в тому числі дані, що стосуються антикорупційної тематики (див. Додаток А.3).

2.4.YOUTUBE_DOWNLOADER є продовженням попереднього скрипту, що орієнтований на збір даних по цільовим YouTube-каналам, що дозволяє робити більш ґрунтовний аналіз відео-контенту (див. Додаток А.4).

2.5.VIDEO_DOWNLOADER – інструмент для автоматизації завантаження відеофайлів з YouTube у форматі AVI, MOV або MP3 за допомогою застосунку yt-dlp ("YT-dlp"), що надає можливість не лише зберігати відео для перегляду, а й використовувати отриманий матеріал для подальшого аналізу (контент-аналізу, візуального аналізу тощо) (див. Додаток А.5).

2.6.TRANSCRIBATOR – інструмент для автоматизації стенографування аудіо- та відеозаписів із використанням API AssemblyAI ("AssemblyAI Documentation"). Сервіс дозволяє працювати з англо-, німецько-, франко-, російсько-, україно- та іншомовними матеріалами (див. Додаток А.6).

2.7.TRANSLATOR – скрипт-перекладач, що функціонує на основі API OpenAI ("OpenAI developer platform"). Він забезпечує автоматизований переклад великих обсягів тексту між українською, англійською та російською мовами, що

значно розширює аналітичні можливості у багатомовних дослідженнях (див. Додаток А.7).

2.8.SANCTIONS_CHECK – застосунок, що дозволяє перевіряти фізичних та юридичних осіб на наявність у санкційному списку Ради національної безпеки і оборони України. Логіка коду полягає в наступному: користувач вводить ПІБ або найменування організації, після чого скрипт проводить звірку з офіційним реєстром санкцій. У разі виявлення збігу система видає дані про дати внесення до списку та дати зняття санкцій, а також інші релевантні відомості (див. Додаток А.8).

4. Експериментальні розробки.

До цієї категорії публікації відносяться ті, що містять в собі результати безпосереднього застосування інноваційних аналітико-статистичних технологій як інструменту для виявлення суб'єктів корупційних відносин або оцінювання безпосереднього рівня корупції. Так, в дослідженні (Ralha & Silva, 2012) Бразильського університету та CGU (Controladoria-Gereldaunião (CGU) – орган федерального уряду Бразилії, який був створений у 2001 році, що відповідає за безпосередню допомогу Президенту в питаннях щодо захисту державної власності, проведення аудиту, забезпечення прозорості та протидії корупції) описується проблема отримання корисної інформації з метою протидії корупції з федеральної бази закупівель у Бразилії, яка використовується державними аудиторами для виявлення та запобігання картельної корупції (змов).

Основними перешкодами виявлення корупції, на думку авторів, є велика кількість даних, що використовуються для вивчення відносин, а також динамічні та диверсифіковані стратегії, що використовуються компаніями для приховування їх шахрайських схем та операцій. Для вирішення цих проблем було розроблено аналітико-статистичну технологію ідентифікації картельних змов в системі державних закупівель під назвою AGMI (від "agent-mining"), де було використано такі методи як розподілений аналіз даних (distributed data mining – DDM), виявлення знань у базах даних (knowledge discovery in data bases – KDD), багатоагентні системи (multi agent systems – MAS) та інші

технології розподільних обчислювань (сітка, хмара тощо), які включені в концепцію інтелектуального програмного агента (intelligent software agent – ISA) (див. рисунок 3.7).

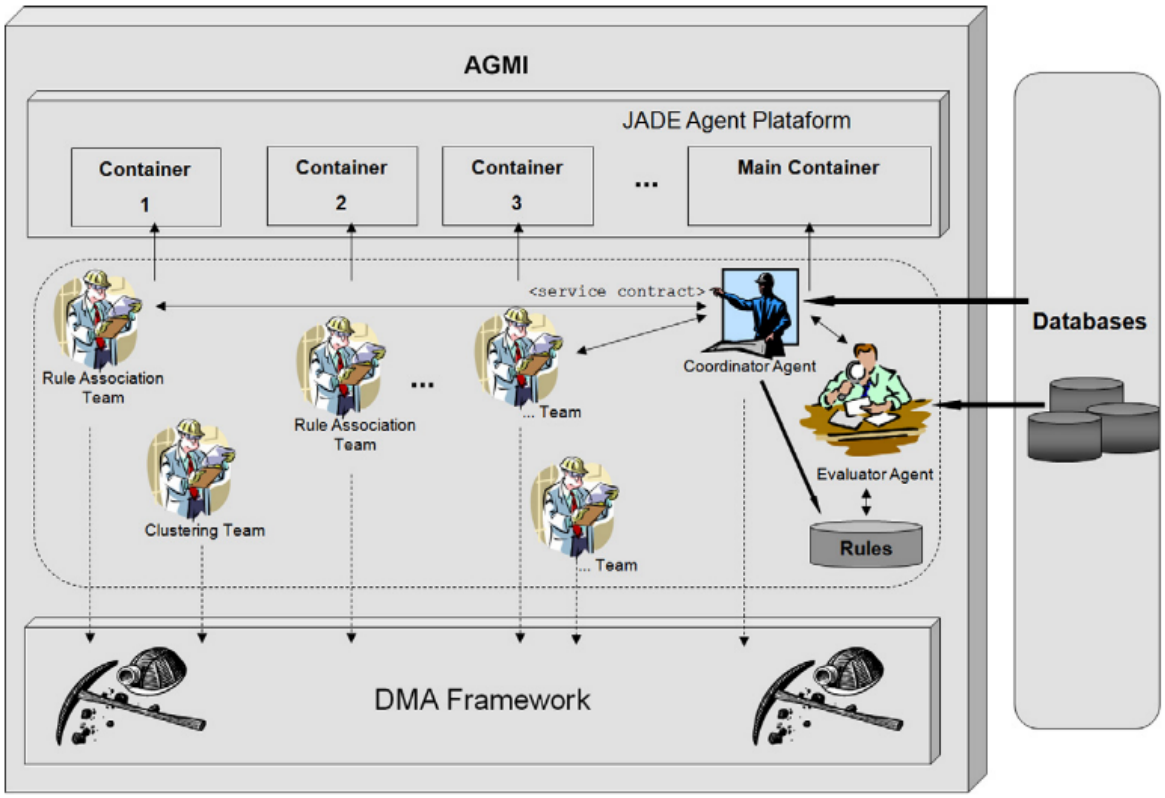

Рис. 3.7 – Архітектура AGMI на платформі JADE
(Ralha & Silva, 2012, p. 11648)

У дослідженні автори поєднали два методи аналізу даних – DDM/KDD та MAS. За допомогою першого інструменту дослідники виявили необхідну первинну інформацію, а завдяки другого групували взаємодіючих агентів, що беруть участь у закупівлі, що дозволило авторам виявити приховані форми корупційних схем. Так, у дев'яти різних державних закупівлях, здійснених в одному і тому же штаті для однієї державної установи, алгоритм виявив процес закупівель за участю двох компаній, одна з яких вигравала усі тендерні конкурси. Дослідники звернули увагу на той факт, що програшна компанія більше не брала участь у жодних покупках, але діяла лише свого роду спаринг-партнера для переможця. Це було свідченням можливого моделювання конкуренції для маскування створення картелю. Підставна компанія, ймовірно, була створена

лише для того, щоб імітувати конкуренцію в державних закупівлях, в яких конкуренція є обов'язковою. Автори дослідження показали, як система дозволяє не лише ефективно групувати дані про державні закупівлі, але й виявляти більше прихованих механізмів, що імітують конкуренцію на користь картельних змов.

До цієї ж категорії можна віднести дослідження (J. Liu et al., 2015). Як стверджують автори цієї публікації, організована злочинність в США змінила стратегію своєї діяльності щодо продажу наркотиків, а саме відійшла від практик нелегального розповсюдження і почала займатися менш ризикованими видами діяльності в сфері охорони здоров'я. Національна асоціація охорони здоров'я з боротьби з шахрайством (NHCAA) повідомила, що лише у Флориді державні та приватні програми медичної допомоги втратили сотні мільйонів доларів у зв'язку із діяльністю організованої злочинності, в ході якого деякі співробітники медичних установ стають учасниками шахрайських та корупційних схем, включаючи виписування непотрібних рецептів, отримання відкатів тощо. Також учасниками змов інколи стають і пацієнти. Дослідження авторів презентує результати розробки аналітико-статистичного методу аналізу даних із використанням методу аналізу графів в сфері охорону здоров'я з метою пошуку шахрайської (корупційної) чи зловмисної поведінки.

Автори методу, за підтримки фахівців консалтингової та аудиторської компанії Xerox Services, розробили програму перевірки доброчесності – Xerox Program Integrity Validator (XPIV), що була застосована в роботі аналітиків компанії Xerox під час проведення аудитів та слідчої діяльності. Програма дає можливість: 1) автоматизувати процес створення переліку (звуження кола) підозрюваних контрагентів (automated screening); 2) отримати початкові дані про подію чи особу, які викликали у системи підозру, з можливістю прослідкувати взаємозв'язок та зібрати докази для побудови слідчої справи (interactive drill down). «Автоматизований скринінг» фокусується на визначенні оптимального алгоритму (методу) виявлення аномалій, а «інтерактивне буріння» фокусується на індексації баз даних для забезпечення швидкого пошуку даних та створенні

інтерфейсу користувача для інтуїтивної взаємодії користувача з інформаційною системи.

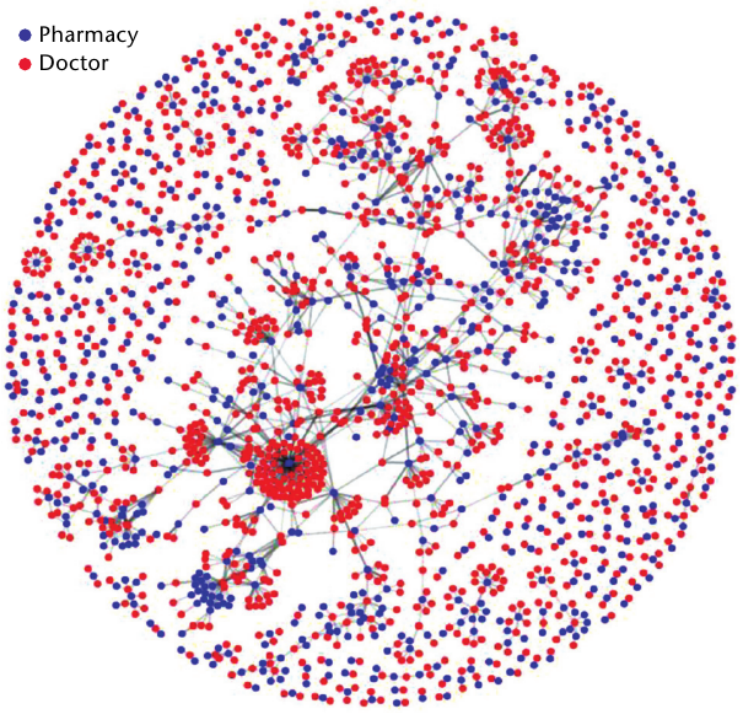

Рис. 3.8 – Дводольний граф (J. Liu et al., 2015)

За твердженням авторів, XPIV є першою інформаційною системою, що дозволяє аналітикам в сфері шахрайства та корупції виявляти мережеве шахрайство (network-based fraud) або коротше кажучи, корупцію, атрибутивною характеристикою якої є не лише участь посадової особи в шахрайській схемі, а наявність змови з іншою (третьою) стороною. Кожен набір даних представлений як великий, гетерогенний граф, де вузли представляють мільйони пацієнтів і сотні тисяч провайдерів (лікарів, лікарні, аптеки), а ребра представляють мільярди затребуваних послуг, медикаментів і поставок, пов’язаних з множинами відносин між ними. Система шукає чотири типи аномалій в графах: 1) підозрілі особи; 2) підозрілі відносини; 3) аномальні тимчасові зміни та геопросторові характеристики, і 4) структури.

Існує два підходи до аналізу графів. Перший, відомий як егоцентричний підхід (ego-net), фокусується на окремих вузлах і особливостях розподілу зв’язків з іншими вузлами (див. рисунок 3.8). Цей підхід дозволяє досліджувати

відносин, пов’язані із отриманням наркотичних засобів, отримувати просторово-часові характеристики потоку пацієнтів між аптеками і лікарями чи лікарнями. Другий підхід аналізує глобальну структуру мережі охорони здоров’я і шукає спільноти, що мають спільні ознаки підозрілої (шахрайської) поведінки, або ті об’єднані спільноти, що набувають рис аномальності за умов аналізу агрегованих даних (див. рисунок 3.10). Саме структурний підхід дозволяє ідентифікувати шахрайські (корупційні) мережі, такі як мережі змов або організовану злочинність.

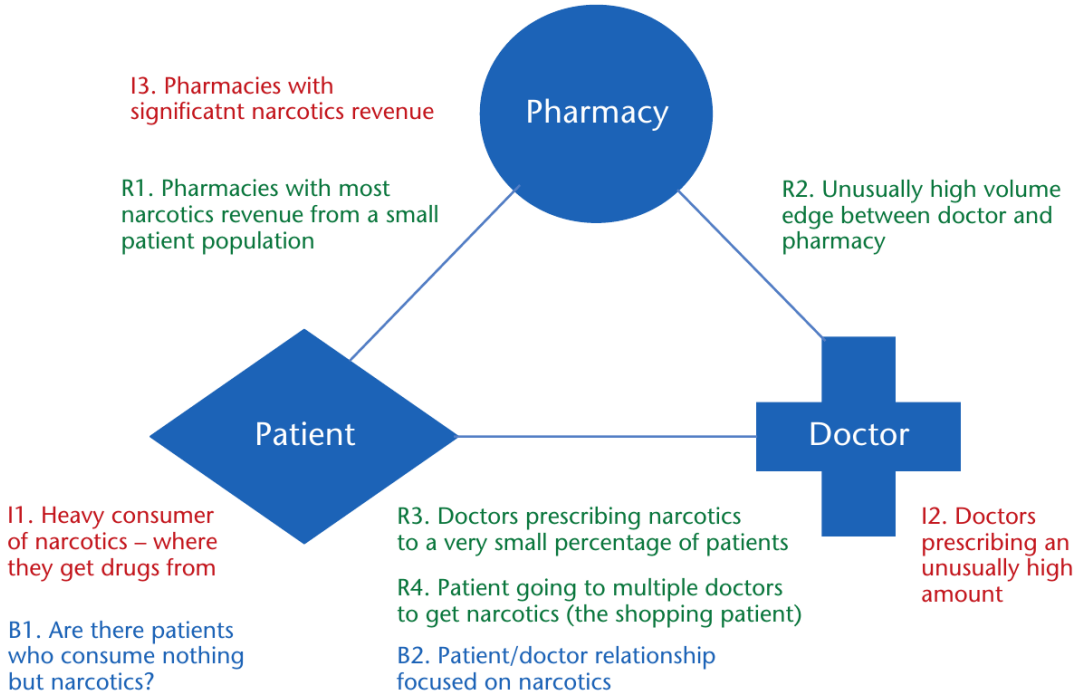

Рис. 3.9 – Аномалії в графах відносин, пов’язаних із наркотичними речовинами (J. Liu et al., 2015)

На рисунку 3.9 наведено перелік різних аномалій, які можна знайти у графах відношень. Аномалії діляться на три категорії: аномалії індивідуального рівня (з міткою I), аномалії зв’язки (edge) (з міткою R) і аномалії з недослідженою медичною поведінкою (з міткою B). Вони показані в різних відтінках сірого або (якщо в кольорі) червоного, зеленого і синього шрифтів відповідно. Аналіз індивідуальних аномалій передбачає: аналіз осіб, віднесених до категорії «тяжкі споживачі наркотичних речовин» та джерел отримання ліків (I1); лікарів, що

призначають багато наркотичних речовин і кому саме (I2); аптеки, що продають багато наркотичних речовин і кому саме (I3). На ці питання легко відповісти, виходячи зі степенів і вагових особливостей.

Аномальні відносини можуть включати незвично сфокусовані відносини, коли: (R1) продаж наркотичних засобів аптеками здійснюється обмеженій кількості пацієнтів чи згідно рецептів обмеженого кола лікарів; (R2) лікар направляє виписує рецепт на придбання важких наркотиків в певні аптеки; і (R3) лікар призначає наркотики лише декільком пацієнтам. Висока концентрація між вузлами може бути інтерпретована як потенційна змова.

Наслідком такого аналізу є здатність швидко виявляти шахрайські схеми, які представляють інтерес для певних слідчих органів. Наприклад, система ідентифікує так званих «торгових пацієнтів» (R4), тобто пацієнтів, що відвідують велику кількість лікарень, лікарів з метою отримання рецептів на ліки із наркотичними речовинами.

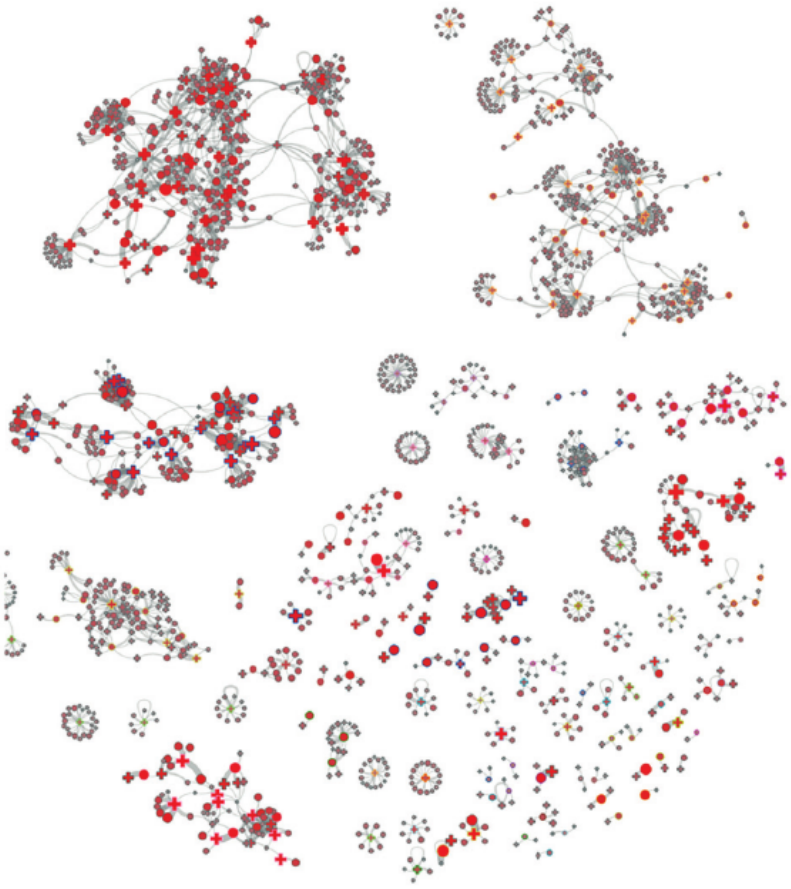

Рис. 3.10 – Аномальні спільноти, виявлені системою (J. Liu et al., 2015)

Поведінкові аномалії – це ті патерни поведінки, які важко пояснити в рамках медичної практики. До них відносяться пацієнти, що споживають нічого, окрім наркотиків (B1); або відносини пацієнт-лікар зосереджується на виписуванні рецептів лише на наркотичні ліки. Для кількісної оцінки показників здійснюється додатковий аналіз даних наданих лікарем пацієнту рецептів, що не включають наркотичні речовини, з метою визначення співвідношення та можливого факту приховування змови.

Окремим прикладом експериментальних розробок можна вважати дослідження в сфері електоральної корупції. В англомовній літературі статистичні методи, що покликані вирішити перелічені вище проблеми, називаються «electoral forensics», що можна перекласти як «електоральна криміналістика». При цьому електоральну криміналістику можна розуміти у двох значення. В широкому значенні, електоральна криміналістика включає в себе такі методи, як паралельний підрахунок голосів, спостереження за ходом голосування або перерахунок вибірки з бюлетенів після голосування, які важко назвати суто аналітичними чи статистичними методами. У вузькому значенні електоральна криміналістика передбачає орієнтацію на аналітико-статистичні методи з мінімізацією людського чинника та оперування усіма даними загалом. Використання аналітико-статистичних методів в електоральній криміналістиці засновано на використанні принципу нормальності (Hicken & Mebane, 2017).

У вузькому розумінні електоральна криміналістика включає дві основні групи методів. Перша базується на числовій теорії та зосереджена на аналізі частотних властивостей електоральної статистики. Друга ж орієнтується на виявлення аномалій у взаємозв’язках між ключовими параметрами виборчого процесу, такими як співвідношення між явкою виборців і рівнем підтримки кандидатів.

На думку А. Подлазова (Кудінов & Яцина, 2025), існує чотири прості статистичні тести, які різняться мірою обґрунтованості, надійності, аналізованими ознаками і рівнем вибірковості. Поєднання цих тестів дає різнобічне уявлення про форми та масштаби фальсифікацій: 1) тест на

переважання круглих чисел; 2) тест на згустки; 3) тест на жадібність; 4) тест (аналіз) недійсних бюлетенів. Найчастіше об’єктом фальсифікації стають такі електоральні характеристики як 1) кількість виборців, які взяли участь у виборах; 2) явка виборців – частка зареєстрованих виборців, які взяли участь у виборах (які отримали бюлетень); та 3) результат влади – частка виборців, які підтримали партію/кандидата влади, що вимірюється від кількості тих, хто взяв участь у голосуванні.

Основним критерієм, що використовується для виявлення фальсифікацій, є розбіжність реальних (документально зафіксованих) результатів виборів від нормативних (модельних).

У першому випадку у якості нормативної моделі виступає певний розподіл цифр, що очікується від «спонтанного» фіксування волевиявлення виборців, у другому випадку – певні відносини між загальними параметрами виборів (зазвичай – явкою) та приватними (зазвичай – частками голосів, поданих за кандидатів чи партії).

В основі першої групи методів були спроби застосувати закон Бенфорда до аналізу електоральних даних. Цей закон стосується розподілу перших кількох цифр великих номерів. Виходячи з цього закону, чисел, що починаються з одиниці, завжди зустрічається більше, ніж чисел, що починаються з двійки. Кількість номерів, що починаються на цифру два, завжди більше чисел, що починаються на з цифру три, і т.д.: 3>4, 4>5, 5>6, 6>7, 7>8, 8>9.

Найважчою формою фальсифікації результатів є їхнє вигадування, коли числа у виборчих протоколах не перебувають у будь-якому зв'язку зі вмістом урн. Оскільки люди не можуть ефективно створювати випадкові числа, існує значна ймовірність, що цифри, які людина вигадує сама, не будуть відповідати закону Бенфорда (див. рисунок 3.11, 3.12). За такого грубого підходу в «результатах» переважають психологічно привабливі числа. Логіка застосування закону Бенфорда полягає в тому, що при появі цифр у протоколах, обраних людиною як «випадкові», ймовірність призначити останньою цифрою «круглу», наприклад, 5 або 0, буде вищою, ніж «незручну», наприклад, 8.

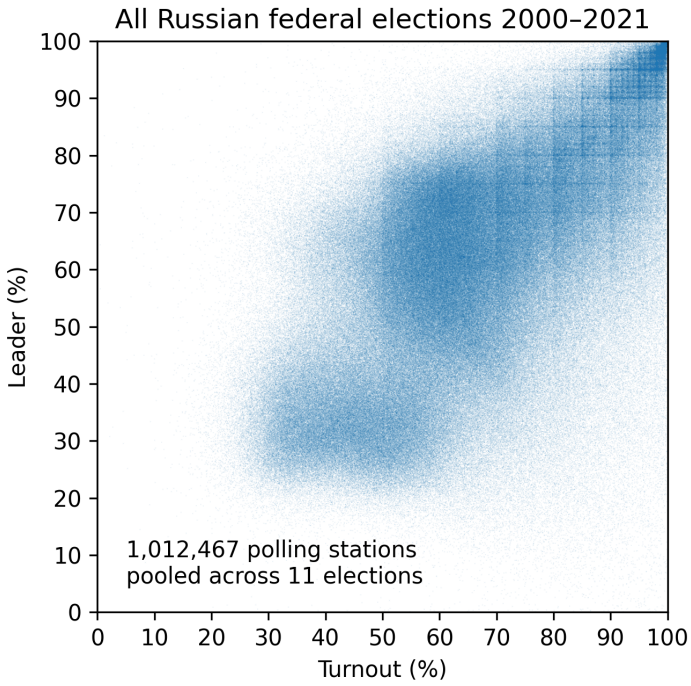

Рис. 3.11 – Прояви закону Бенфорда на візуалізації даних результатів виборів/референдуму у вигляді точкової діаграми (візуалізація автора на основі (Kobak et al., 2020; "Statistical Anomalies in Russian Elections," 2024))

І, аналогічно при штучному отриманні електоральних даних ймовірність зустріти парні цифри у молодших розрядах (11, 22, 33...) відрізнятиметься від очікуваної ймовірності у 1/10. Цей метод зазвичай називають методом Бебера і Скакко (Beber & Scacco, 2012; Кудінов & Яцина, 2025).

Друга група методів здійснює пошук аномальних залежностей між загальними (явкою) і приватними (успіх конкретного партійного списку або кандидата) показниками електоральної статистики із застосування методу моделювання.

Крім вигадування чисел існує ще один механізм фальсифікації, що сприяє виникненню круглої кількості виборців, які взяли участь у виборах – кількість виборчих бюлетенів, одержаних дільничною виборчою комісією, найчастіше саме закінчується на «0», оскільки їх відраховують десятками. Виникає ефект жадібного голосування – ситуація, коли кількість виборців, які взяли участь у виборах, точно збігається з числом бюлетенів, отриманих дільничною виборчою

комісією, але при цьому виявляється меншою за кількість виборців, зареєстрованих у її списках (Yatsyna & Kudinov, 2023, p. 36).

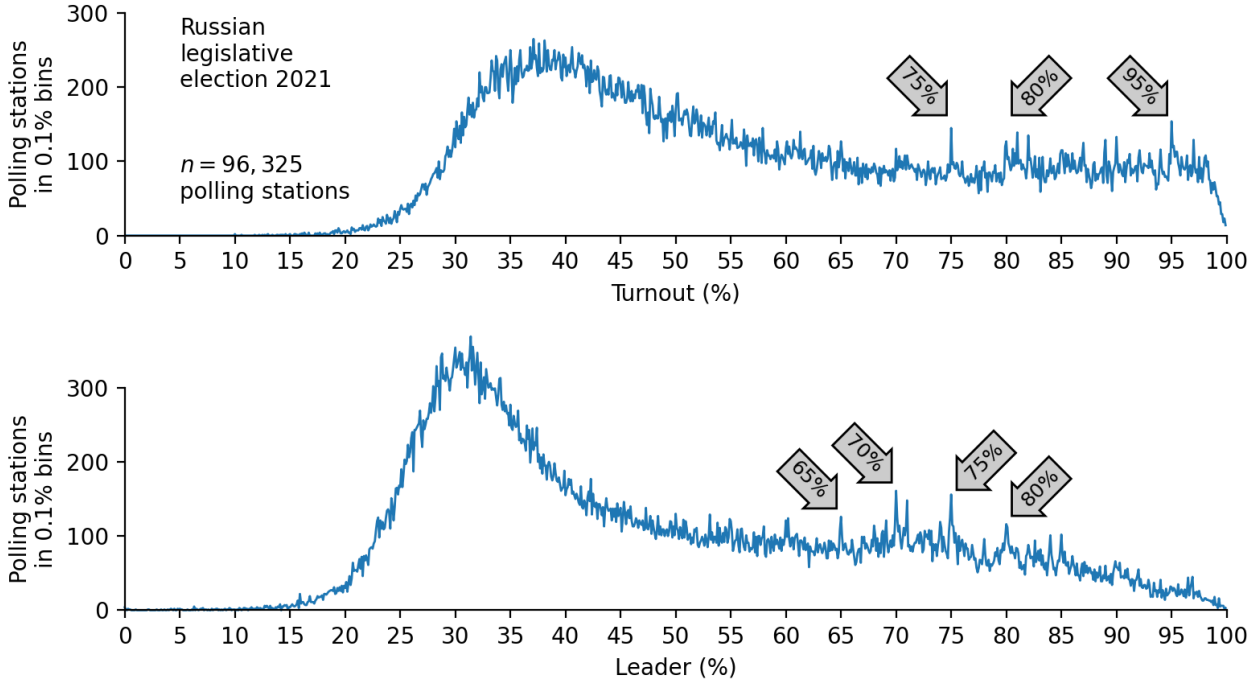

Рис. 3.12 – Прояви закону Бенфорда на візуалізації даних результатів явки і голосування за переможного кандидата/партію у вигляді лінійного графу (візуалізація автора на основі ("Statistical Anomalies in Russian Elections," 2024))

Якщо звернутися до результатів науково-дослідної роботи Мічиганського університету (Hicken & Mebane, 2017), існує три напрямки розвитку моделей оцінки результатів виборів, що дозволяють отримати статистично обґрунтовані висновки щодо електоральних фальсифікацій.

1. Першою можна вважати модель мультимодального шахрайства (Klimek et al., 2012). Згідно з концепцією авторів, базове припущення полягає в тому, що голоси на виборах без шахрайства формуються через взаємодію процесів, ефекти яких можна узагальнити за допомогою двох нормальних розподілів: одного розподілу для часток явки та іншого, незалежного розподілу для частки голосів на користь «переможця» (тобто партії з найбільшою кількістю голосів). Автори припускають, що електоральне шахрайство – це ситуація, під час якої здійснюється збільшення кількості голосів за переможця із порушенням

офіційних процедур голосування. Деякі голоси переносяться до переможця від опозиції, а деякі – від тих, хто не з'явився на виборчу дільницю. При цьому автори виділяються два види електорального шахрайства: поміркування ("incremental") та жадібне ("extreme"). В першому випадку перенос голосів здійснюється обережно; в другому – перенос здійснюється для всієї загальної чисельності виборчої дільниці без додаткових розрахунків щодо тих голосів, які дійсно відбулися.

Автори тестували заявлені статистичні характеристики результатів голосування (і їх відхилення) в крос-національних умовах на різних рівнях агрегування даних. В якості центральної точки була запропонована параметрична модель статистичної оцінки вірогідності вкидання бюлетенів, яка, можливо, вплинула на результати виборів. В пізніших публікаціях метод був перероблений: для опису виборів стали використовуватися двомірні гістограми, де по одній з осей відкладаються відсоткові частки явки, по іншій – частка параметра, що цікавить дослідника (зазвичай – відсоток голосів, набраний переможцем), а насиченість кольору точок на площині відображає число спостережень, що описуються відповідним набором значень, що автори називають «відбитками» електоральної системи.

У роботі (Klimek et al., 2012) за допомогою математичної моделі було продемонстровано, що ефект «діагонального розмиття» області значень на гістограмі є наслідком фальсифікацій із вкиданням бюлетенів / передачею бюлетенів від однієї партії до іншої. Такий ефект був виявлений у виборах 2011 та 2012 років в Російській Федерації, а також в Уганді у 2011 році (див. рисунок 3.13).

Було розраховано критичні значення параметрів, що визначають ймовірність того чи іншого варіанту шахрайства: f_i – це ймовірність поміркованого шахрайства, а f_e – ймовірність жадібного шахрайства. Інші параметри повністю описують бімодальні та тримодальні розподіли, які модель характеризує як наслідки електоральних шахрайств.

Похідною від даної моделі є її модифікація із визначенням показника ймовірності шахрайства на рівні вибіркової дільниці. В даному випадку увага акцентується на 1) статистичних тестах щодо наявності шахрайства та 2) оцінках ймовірності того, що кожна спостережувана одиниця агрегації голосів – наприклад, кожна дільниця – є шахрайською (Mebane & Wall, 2015).

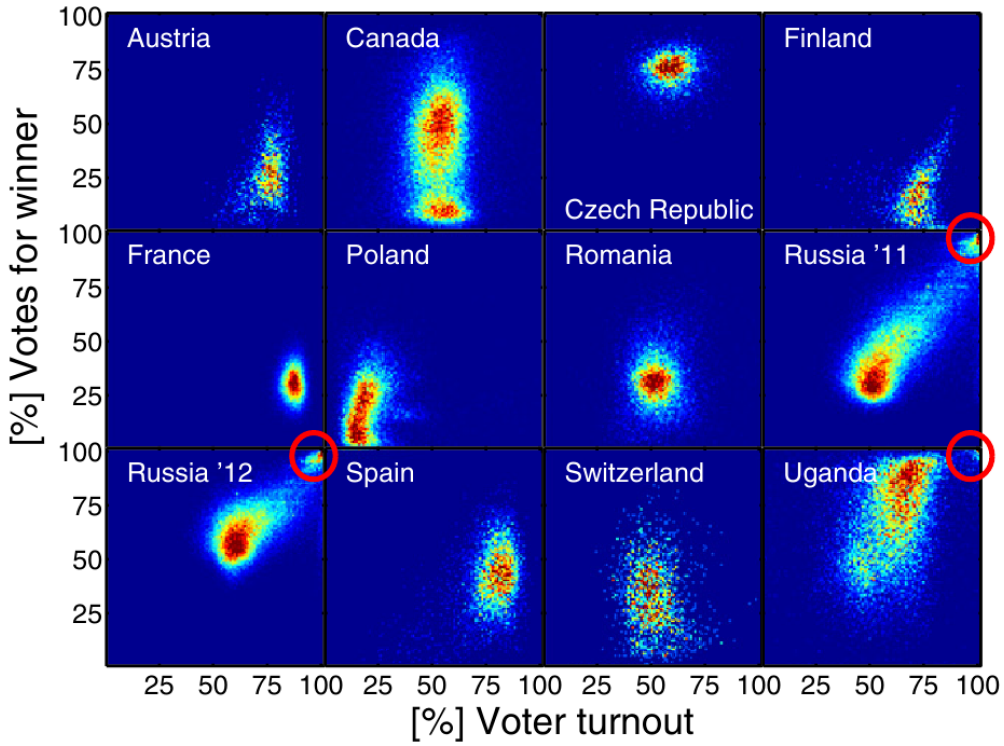

Рис. 3.13 – Візуалізації «виборчих відбитків» за результатами пошуку аномалій в даних результатів парламентських виборів різних країн (Klimek et al., 2012)

2. Для вирішення недоліків попередньої моделі виникла модель географічної кластеризації (див. (Yatsyna & Kudinov, 2023)). Індикатори чи явища, які географічно кластеризовані, заслуговують особливої уваги. Географічна кластеризація може показати, де відбувається співпраця або змова під час виборчого процесу. Географічна кластеризація також може натякнути тим, хто має відповідні експертні знання, на інші фактори, які можуть сприяти спостережуваним шаблонам у виборчих результатах. Ці інші фактори можуть бути пов'язані або непов'язані з можливістю шахрайства. Наприклад, кластер може збігатися з домашньою базою політичного лідера або з територією, на якій переважає політична партія або етнічна група лідера (або меншості). Виходячи з

цього методу, використання географічних координат дозволяє отримувати додаткові підтвердження про втручання в електоральний процес. У найбільш простому вигляді як така функція передбачається залежність від відстані між географічними точками: чим ближче розташовані виборчі дільниці (і, отже, чим ближче один до одного живуть виборці, що голосують на них), тим менше має бути відмінність у результатах голосування на цих дільницях.

На відміну від попередніх моделей, робота з географічними даними передбачає набагато більші трудовитрати при неясних перспективах дослідження. Без чіткого уявлення про географічні властивості електорату складно виправдати витрати на з'ясування адрес виборчих дільниць і тим більше зіставлення їх з географічними координатами. З урахуванням можливостей новітніх інформаційних технологій, цей метод може мати значний розвиток в разі впровадження технологій електронного голосування, що не за горами.

3. Третя модель є поєднанням попередніх двох і представлена не лише у вигляді публікацій, а у вигляді онлайн-сервісу «Інструментарій електоральної криміналісти» (Election Forensics Toolkit) (Mebane & Kalinin, 2023), що дозволяє кожній зацікавленій особі здійснити статистичне оцінювання власних масивів електоральних даних, або подивитися на роботу із наявними в системі даними.

Інформаційна система оцінює масиви за такими тестами: 2BL, LastC, C05s, P05s, Skew, Kurt, DipT. 2BL – тест середнього значення другої цифри. «Друга цифра» відноситься до другої значущої цифри в кожному підрахунку, до якого застосовується тест (наприклад, якщо підрахунок становить «1234», то «2» є другою значущою цифрою). LastC – тест середнього значення останньої цифри. «Остання цифра» відноситься до останньої цифри в кожному підрахунку, до якого застосовується тест (наприклад, якщо підрахунок становить «1234», то «4» є останньою цифрою). C05s – тест середнього значення бінарної змінної, яка вказує, чи є остання цифра підрахунку голосів для відповідної партії або кандидата нулем або п'ятіркою. P05s – тест середнього значення бінарної змінної, яка вказує, чи є остання цифра округленого відсотка голосів для

відповідної партії або кандидата нулем або п’ятіркою. Skew – тест на асиметрію. Kurt – тест на ексцес. DipT – тест на унімодальність.

Слід зазначити, що жоден із проілюстрованих методів неспроможний однозначно підтвердити факт фальсифікації виборів. Вони можуть лише вказувати на наявність аномалій даних і порушувати питання про подальше розслідування. Рішення про те факт фальсифікації виборів приймається відповідними органами влади і має ґрунтуватися на додаткових дослідженнях та доказах.

Тим не менш, є прецеденти, коли використання алгоритмів пошуку аномалій на виборах призводило до виявлення фактів фальсифікації у 2009 році в Ірані. Фахівці, що проводили аналітико-статистичний аналіз результатів голосування в Ірані констатували відносну перемогу Махмуда Ахмадінежада, щоправда, зробили вони це дуже обережно. Н. Сілвер порівняв результати Махмуда Ахмадінежада у 2009 році з результатами першого туру 2005 року кандидатів від консервативного табору (Ахмадінежад, Ларіджані та Галібафа) та виявив деякі розбіжності. Наприклад, у провінції Луристан у 2005 році кандидати-консерватори отримали лише 20% голосів, а у 2009 році 71% виборців проголосували за Махмуда Ахмадінежада. У Тегерані, навпаки, підтримка представників правого табору в 2009 році зменшилася порівняно з 2005 роком. Загалом по країні кореляція між результатами 2005 і 2009 років все-таки була присутня, але у слабкій формі. Тому Н. Сілвер не став робити однозначного висновку про фальсифікації, оскільки переваги виборців могли змінюватися з часом (Silver, 2009).

Деякі дослідники проаналізували вибори в Ірані через закон Бенфорда. Такий аналіз стосовно президентських виборів в Ірані провів В. Мебане (див. рисунок 3.14). Він дійшов висновку про існування статистичних спотворень у підрахунку голосів, відданих за Мехді Кяррубі та Мохсена Резаї, у бік зменшення. Також ним було знайдено статистичні невідповідності у результатах Махмуда Ахмадінежада у бік збільшення поданих за нього бюлетенів. Але дані Мір-Хосейна Мусаві, на його думку, були вірними. Мебане зробив висновок, що

якщо і була фальсифікація підсумків голосування, то вона полягала у відборі голосів у Кяррубі та Резаї та передачі їх Ахмадінежаду. У цьому випадку ймовірним був другий тур голосування, хоча даних, що точно підтверджують це твердження, у розпорядженні Мебане не було (Mebane, 2009).

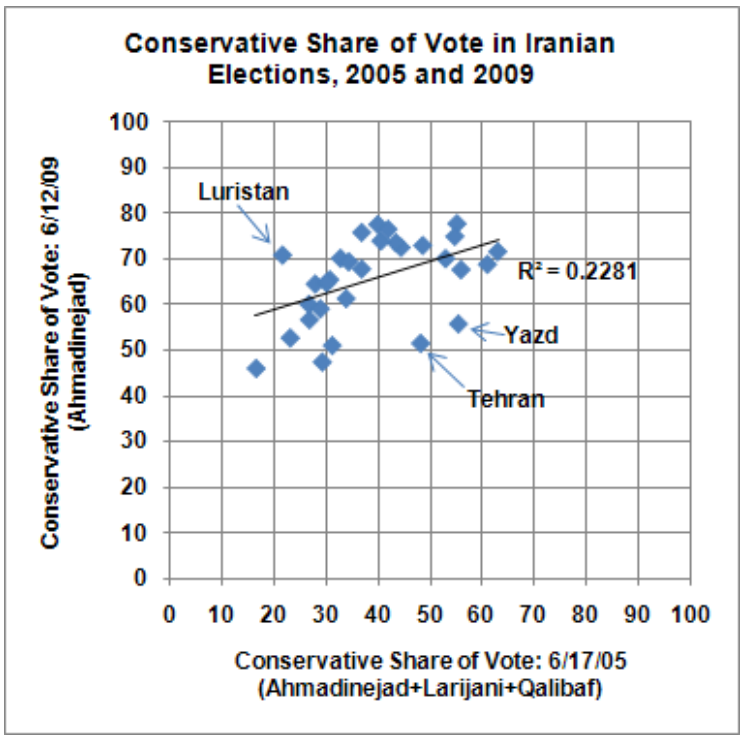

Рис. 3.14 – Графік порівняння між відсотками голосів, які Ахмадінджад отримав у 2009 році з відсотками голосів, отриманими консервативними кандидатами (Ахмадінежад, Ларіджані та Галібафа) у першому турі виборів 2005 року (Silver, 2009)

Також він виявив закономірність, яка полягає в тому, що чим більше голосів набирав Махмуд Ахмадінежад на виборчих дільницях, тим менше там було зіпсованих чи недійсних бюлетенів. Щодо Мір-Хосейну Мусаві такої динаміки не спостерігалося. Найпростішим поясненням цієї закономірності може бути вкидання бюлетенів за Ахмадінежада чи якась інша дія, що штучно додає голоси до його результатів. В результаті, Мебане дійшов висновку, що у такий спосіб частка чинного президента в офіційних результатах голосування могла збільшитися на 5% (Mebane, 2009).

Загалом, використання алгоритмів пошуку аномалій в даних електоральної статистики може бути важливим інструментом виявлення дійсних фактів фальсифікації виборів. Однак, як зазначають дослідники, необхідно застосовувати їх з обережністю та аналізувати отримані результати у поєднанні з іншими джерелами інформації, оскільки, як показує сумнівна практика, статистичні розрахунки, що не підкріплені додатковими доказами, можуть розцінюватися зацікавленими особами, наприклад в ситуації національних виборів, не як інструмент попередження / протидії корупції, а лише як засіб делегітимації результатів виборів із відповідними наслідками і реакцією влади/опозиції.

Отже, впровадження інноваційних аналітико-статистичних технологій попередження / протидії корупції в державі можна розділити на 4 напрямки:

– методологічний напрям – в якому дослідники розробляють універсальні методи (алгоритми) аналізу даних (пошуку аномалій) із визначенням можливих сфер їх практичного застосування, в тому числі і в сфері попередження / протидії корупції;

– напрям вторинного аналізу даних – в якому автори намагаються розробити власні показники рівня корупції або описати стан розвитку корупційних відносин у певний період часу на базі існуючих показників;

– напрям створення автоматизованих систем аналізу текстових даних – в якому відображаються результати впровадження технологій NLP (обробки природньої мови) у поєднанні з технологіями просторової візуалізації даних;

– роботи, що присвячені результатам практичного впровадження технологій машинного навчання і штучного інтелекту для ідентифікації суб’єктів корупційних відносин та/або отримання статистично обґрунтованих підтверджень наявності / відсутності корупції.

Найбільшу значимість в даному випадку мають практико-орієнтовані дослідження, адже саме на цьому рівні відбувається безпосередня апробація відповідних теоретичних моделей і методологічного інструментарію, а також створюються прецеденти для використання результатів аналітико-статистичних

досліджень як складової доказової бази тих або інших фактів шахрайства або корупції.

Висновки до підрозділу логічно почати з того, що впровадження інноваційних аналітико-статистичних технологій як інструменту попередження / протидії корупції потребує подвійної стратегії: зверху вниз і знизу вгору. З одного боку, ми бачимо необхідність законодавчого підкріплення, що задає рамки для розвитку інституційних рішень, а з іншого – мобілізацію громадянського суспільства та використання його потенціалу як активного наглядача за діями держави. Ефективність сучасних технологічних рішень у боротьбі з корупцією прямо залежить від того, наскільки гармонійно ці дві стратегії інтегруються між собою, створюючи єдине поле для дій. Приклади таких інтеграцій, як Kalsada на Філіппінах чи Dozorro в Україні, демонструють реальні результати, що доводять перевагу машинного аналізу перед ручними аудитами, особливо коли йдеться про великі масиви даних.

Надзвичайно важливо підкреслити, що аналітико-статистичні дослідження розвиваються за кількома ключовими напрямами, які не тільки взаємодоповнюють один одного, але й формують цілісну екосистему боротьби з корупцією. Аналіз вторинних даних дозволяє створювати прогнозні моделі, що ґрунтуються на історичних індикаторах, тоді як автоматизовані системи аналізу текстових даних розширюють горизонти, додаючи до кількісних вимірів змістовні та просторові характеристики. Методологічні розробки, своєю чергою, забезпечують теоретичну базу, яка підтримує практичні експерименти, формуючи надійні алгоритми виявлення аномалій. Зрештою, експериментальні розробки показують, як ці інструменти можуть впливати на конкретні процеси і ситуації, і створюють підґрунтя для масштабування рішень.

Особливої уваги заслуговує те, що значна частина інноваційних рішень, які апробуються в антикорупційній сфері, мають міждисциплінарний характер, поєднуючи технології аналізу часових рядів, графових структур, а також штучного інтелекту. Це дозволяє ефективно працювати не лише з числовими, але й з поведінковими, структурними та географічними даними. Практичні

приклади, зокрема в сфері охорони здоров’я чи державних закупівель, демонструють, як машинне навчання може допомогти виявляти змови, шахрайські схеми й картелі навіть у складних мережах взаємодій. Інтеграція таких рішень у державні системи стає не просто технічним питанням, а стратегічним, оскільки від їхньої надійності залежить репутація і довіра до інституцій.

Слід також підкреслити важливість експериментальних досліджень у реальних умовах, що підтверджують гіпотези і моделі, які були розроблені в теоретичному або лабораторному середовищі. Електоральна криміналістика тут є особливо яскравим прикладом: методи на кшталт аналізу закономірностей Бенфорда чи мультимодальних моделей шахрайства дозволяють не лише виявляти аномалії, але й ставити важливі питання перед суспільством про чесність і прозорість виборчих процесів. Водночас результати численних досліджень показують, що жоден статистичний метод не може дати остаточний вердикт про фальсифікації, а лише вказує на потребу в подальших розслідуваннях, поєднуючи кількісні та якісні підходи.

3.3. Практичні рекомендації щодо впровадження інноваційних аналітико-статистичних технологій попередження корупції в Україні

В цьому підрозділі ми сконцентруємо нашу увагу саме не на практичних рекомендаціях, а скоріше на застереженнях щодо занадто оптимістичного сприйняття, як інформаційних, так і аналітико-статистичних технологій в якості панацеї від усіх корупційних хвороб.

Почнемо з того, що не всі представлені в роботі результати досліджень чи спроб створити цифровий інструмент для боротьби з корупцією в державі побудовані на аналізі об’єктивної інформації, тобто незалежної від політичної кон’юнктури в тій або іншій країні, в різних географічних куточках країн, на основі даних яких здійснюється той чи інший аналіз (розклад політичних сил та ступінь впливу окремих партій, антикорупційна діяльність виконавчої влади), а також рівня доброчесності дослідників і загального рівня свободи слова в тій або

іншій державі. Наприклад, інструменти, що передбачають проведення аналізу публікацій ЗМІ не завжди можуть відображати справжню картину дійсності, а також не завжди відображати функцію громадського контролю ЗМІ у зв'язку з можливістю навмисного спотворення інформації у висвітленні антикорупційної проблематики. З цього приводу слушною є думка М. Кікалішвілі про те, що «за стандартом останніх десяти-двадцяти років журналістські розслідування та викриття корупційних фактів в Україні дивним чином припадають на час президентських або парламентських передвиборчих гонок (рідше на час проведення тендерів до великих державних замовлень). Всі друковані видання, представники телебачення та радіомовлення, як навіжені починають пістрявити інформацією на будь-який смак. Разом з тим, якщо піддати весь цей об’єм інформації критичному осмисленню, не виникне сумнівів, що більшість матеріалів максимально не об’єктивні. Виборча метушня стає добрим лакмусовим папірцем для визначення того, чи дотримуються серед вітчизняних медіа засади доброчесної журналістики» (Кікалішвілі, 2021, с. 253).

Є багато прикладів «політичної джинси», метою якої є не викривання корупційних схем, отримання конкурентної переваги в бізнесі або політиці. Як відмічає М. Кікалішвілі, замовниками матеріалів є олігархи, політична опозиція або провокатори, де в кожного є власні приховані інтереси. Тому процес створення будь-яких інформаційних систем, що передбачають аналіз публікацій ЗМІ чи навіть систем зворотнього зв’язку має передбачати процедури зіставлення даними, отриманих з інших джерел. Різні методи зворотного зв'язку, створені шляхом збирання скарг та претензій, новинних сайтів, краудсорсингових платформ та соціальних мереж, сприяють як цивільній мобілізації, так і прямій ідентифікації та протидії корупції. Однак, іноді, за активною діяльністю в мережі може бути жодних справжніх дій, а лише театр, вистава, астротурфінг. Астротурфінг (від англ. astroturfing) – це метод маніпуляції громадською думкою, коли організації, групи чи люди намагаються створити ілюзію широкої громадської підтримки або опозиції, якої насправді немає. Це відбувається за рахунок створення фальшивих облікових записів у

соціальних мережах, написання негативних відгуків на конкуруючі продукти чи послуги, купівлі позитивних відгуків на власні продукти чи послуги, написання підтримуючих коментарів на блогах та форумах, організації підтримки чи опозиції у соціальних рухах, мітингах, виборах тощо (Олещук, 2019, с. 319).

Для повного функціонування таких інструментів необхідно, щоб ця інформація була затребувана в тій або іншій країні, або на певній території, а органи державної чи місцевої влади були готові реагувати на отримані повідомлення на засадах принципу рівності будь-яких учасників перед законом та щоб існували законодавчі механізми захисту заявників щодо корупції.

Можна погодитися з думкою про те, що високий рівень розвитку Інтернету впливає на зменшення корупції, але ця умова є важливою, але недостатньою. Здається, що разом із поширеністю Інтернету важливо враховувати наявність інституційних факторів для зменшення корупції та, перш за все, наявності волі протидіяти корупції в державі. Якщо рівень самоорганізації суспільства малий, ідеї про корупцію та механізми протидії їй є найбільш примітивними, а державні органи не проголошують жодного антикорупційного курсу, інституційні заходи боротьби з корупцією (цифровізація державних служб, державних закупівель та інших інструменти) не вводяться, тоді наявність Інтернету не може належним чином забезпечити зменшення корупції.

Зворотним боком цифрової трансформації може стати режим «цифрового концтабору». Термін «цифровий концтабір» зазвичай використовується для опису ситуації, коли люди піддаються масовому спостереженню, контролю та обмеженню прав в інтернеті та цифровій сфері в цілому. Це може включати моніторинг комунікацій, збір персональних даних, цензуру та блокування інформації, а також інші способи обмеження свободи вираження та доступу до інформації. Аналогом даному терміну можна вважати концепцію цифрового (техно) феодалізму (Drahos & Braithwaite, 2002; Varoufakis, 2024; Бабарикіна, 2025). Прецеденти цифрових концтаборів можна знайти у різних періодах історії. Один із таких прикладів – Китайська Стіна Інтернету, яка є системою цензури та

фільтрації інтернет-трафіку в Китаї, обмежуючи доступ громадян до певних сайтів та сервісів (Xu, Mao, & Halderman, 2011).

Необхідно пам’ятати, що цифровізація породжує нові корупціогенні схеми: від торгівлі «великими даними» до махінацій з підрахунком голосів або «випадкових» програмних помилок та збоїв у смарт-контрактах. Сучасні злочинці спроможні створювати застосунки для подолання як закону, так і цифри.

Взагалі, надмірна технологізація може призвести до негативних наслідків. Як зазначав Є. Цокур ще у 2017 році по відношенню до виборчого процесу, технічна досконаліть процедур дедалі частіше слугує не гарантією прозорості, а маскує відхід від базових засад демократії. У гонитві за результатом, перемогою за будь-яку ціну, технологічні інструменти можуть стати частиною політичного інжинірингу, який легітимізує неприйнятні або маніпулятивні сценарії. Автор переконливо показує, що справжня мета виборів – не конфлікт і не перемога, а примирення та суспільна консолідація – дедалі частіше витісняється технологічною логікою оптимізації процесу (Цокур, 2017).

Слід враховувати, що особи, які контролюють цифрові технології, потрапляють у коло потенційних корупціонерів: з відповідними знаннями, компетенціями, навичками для «обходу» наявних засобів протидії. Тому такі особи мають бути на особливому обліку з боку правоохоронних органів.

Не треба забувати і про серйозні корупційні ризики через доступ до великих даних – так звані базові державні інформаційні ресурси включають індивідуальні дані про громадян, відомості економічного характеру, юридичні факти тощо. При цьому персональні дані зберігають найрізноманітніші відомства та організації. Здається, необхідно обмежити законодавчо збирання та зберігання інформації в єдиному сховищі. Таким чином не лише знижується ризик корупційних дій, а й забезпечується інформаційна безпека держави.

Як слушно зазначають І. Чайка та Є. Цокур, новітні технології, наприклад, в електоральному процесі можуть одночасно зменшувати ризики фальсифікацій на етапі підрахунку голосів, але водночас породжують нові етичні виклики,

зокрема пов’язані з крадіжкою ідентичності, а також складністю встановлення відповідальності за вибір, зроблений нібито від імені виборця, але не ним самим. Автори наголошують, що потенційна деперсоніфікація виборчого процесу через технологічні рішення без належного суспільного консенсусу та гарантій справжньої ідентифікації створює нову конфігурацію ризиків, у якій етика перетворюється з допоміжного чинника на головну умову ефективного і справедливого електронного волевиявлення (Чайка & Цокур, 2024).

Якщо говорити про корупційні ризики, то на думку (Расулев & Исмоилов, 2020) до корупційних ризиків впровадження інноваційних інформаційних технологій можна віднести:

– надмірні інвестиції в інформаційні технології, що можуть призводити до зростання корупції, оскільки використання коштів через непрозорий процес закупівель легко створює корупційні можливості;

– технологія blockchain може становити загрозу для антикорупційних зусиль, оскільки це дозволяє проводити повністю анонімно та зашифровано криптовалютні транзакції, які можуть бути використані для розкрадань чи шахрайських операцій;

– електронні ідентифікаційні рішення не є повністю захищеними від хакерів, і урядам необхідно постійно забезпечувати, щоб цифрові рішення, платформи та системи відображали найвищі стандарти безпеки. Це вимагає регулярного оновлення технологій, що може сприйматися обтяженням як громадянами, так і державними службовцями.

– міжнародні стандарти досить узагальнено закріплюють можливість використання високотехнологічних інструментів для попередження / протидії корупції.

Сучасні корупціонери активно використовують новітні технології (криптовалюту) для отримання винагород. Для правоохоронних органів не залишається можливостей використовувати їх як докази, а після того, як віртуальна валюта переміщується за межі України, неможливою стає її конфіскація.

Взагалі, під час впровадження аналітико-статистичних технологій як інструменту попередження / протидії корупції в модель державного управління України необхідно розуміти, що базовими причинами корупції є існуюча в нашій країні модель економіки, що склалася з середини 1990-х років, відсутність ідеологічного обґрунтування соціальної значущості державної служби та орієнтація населення на ідеали суспільства споживання. А отже, корупція в Україні заснована на непереборних цифровізацією підставах та умовах: деструктивним розподілом матеріальних благ у суспільстві та споживацьким світоглядом державного апарату.

Аналіз сучасних тенденцій щодо впровадження інноваційних аналітико-статистичних технологій підтверджує наявність позитивної кореляції між рівнем розвитку інформаційних технологій та рівнем корупції в державі. Однак перспективи та ефективність вищезазначених інструментів для боротьби з корупцією дуже різні, багато з них, якщо вони використовуються, можуть, навпаки, суттєво стимулювати корупційні правопорушення.

Сучасні інформаційно-комп'ютерні технології, забезпечуючи доступ до інформації про події, самі по собі не гарантують публічності (перетворення доступної інформації в усвідомлений факт, що вимагає прийняття управлінських рішень). В результаті виникає розрив між рівнем розвитку суспільства та його інститутами. Досліджені в нашій роботі підходи та реальні кейси застосування інноваційних аналітико-статистичних технологій дозволяють частково протидіяти розвитку корупції в будь-якій державі. Більшість алгоритмів, тестів і методів виявлення корупційних схем надзвичайно прості. Перевірка їхнього теоретичного обґрунтування доступна студентам будь-яких технічних чи математичних (економічних) спеціальностей. Для фахівців зі сфери гуманітарних (історія, політологія, право, соціологія) єдиною перепоною на цьому шляху може стати лише страх перед інформаційними технологіями, на кшталт використання мов R чи Python.

Окремою темою є проблема державних закупівель. Слід розуміти, що існуючі в державі системи контролю мають постійно вдосконалюватися у зв’язку

із появою схем, що дозволяють обійти існуючі обмеження. Наприклад, система державних закупівель «Прозорро» ускладнила розкрадання державних коштів, однак це не вирішило проблему остаточно (Віннічук & Головньов, 2018).

Існує низка способів обходу електронної системи публічних закупівель «Prozorro» (Приходько, 2020, с. 272-274), які, залишаючись у межах формальної законності, на практиці дозволяють реалізовувати корупційні схеми або забезпечувати перевагу «своїм» учасникам. Одним із таких механізмів є складання тендерної документації під заздалегідь визначеного постачальника. Замовник формулює технічні або кваліфікаційні вимоги так, щоб відповідати характеристикам лише конкретної фірми. Це виправдовується посиланнями на потребу в «гарантії якості», оскільки, мовляв, неналежний товар змусить повторювати закупівлю, що потребує додаткового часу й ресурсів. Довести упередженість у цьому випадку практично неможливо.

Поширеною також є практика укладання «додаткових угод» до вже підписаних контрактів. Зовні це виглядає як коригування умов у зв’язку зі змінами на ринку або технічними потребами. Однак саме через такі «додаткові угоди» початкова низька ціна часто зростає до невиправданих рівнів. Формально процедура є легітимною, і навіть найчесніший тендер не завжди обходиться без таких змін, але система створює умови, коли зловживання важко виявити, а обґрунтування перегляду ціни часто носить суто формальний характер.

Інша схема – «неправомірна дискваліфікація», коли замовник, маніпулюючи оцінкою документів, не допускає до участі потенційно вигідного конкурента. Водночас порушення в документах «своїх» учасників ігноруються. Таким чином реалізується практика вибіркової справедливості.

Особливої уваги потребує ситуація, коли учасникам пропонується подати проєкт договору, вже заповнений і підписаний, з включеними наперед «дискримінаційними умовами». Такі умови суперечать принципам ринкових відносин і відсікають реальних представників бізнесу ще на етапі подання пропозиції.

Певна частина тендерів супроводжується «особливими вимогами до переможців», серед яких – максимально розпливчасті характеристики предмету закупівлі, на кшталт «пристроїв із тримачем і насадкою», або ж умови, які можуть виконати лише ті, хто мав завчасну інформацію: короткі строки постачання, необхідність надати документи, які фізично не можна підготувати до моменту торгів.

Судовий тиск також входить до інструментарію тиску. Деякі чиновники ініціюють позови, щоб «блокувати закупівлі в суді». Навіть якщо такі справи не призводять до скасування результатів, вони виснажують конкурента, знижуючи його зацікавленість у продовженні боротьби.

Ще один поширений прийом – участь у торгах «псевдофірм», які навмисне знижують ціну, але після перемоги «відмовляються підписувати договір». У такому разі контракт укладається з наступним учасником або ж тендер оголошується повторно, що відкриває простір для маніпуляцій.

Нарешті, існують випадки, коли оголошення про тендер намагаються зробити малопомітним. Для цього чиновники свідомо спотворюють назву закупівлі (наприклад, «Закупівля машін»), присвоюють їй некоректну категорію, як-от «Електрообладнання, інше», публікують нечітку або нерозбірливу документацію. Таким чином «тендер ховається» в системі, щоб його могли знайти лише «довірені» постачальники, тоді як потенційні конкуренти залишаються не поінформованими.

Ці практики демонструють, що навіть найбільш прозора система може бути адаптована до інтересів корумпованих учасників, якщо немає належного громадського, медіа- та інституційного контролю.

Як зазначає автор (Приходько, 2020, с. 277), для стримування корупції у сфері публічних закупівель необхідна одна ключова умова – наявність політичної волі. Якщо ж вона є, для успіху реформ в означеній сфері необхідно дотримуватися таких ключових принципів: конкуренція, прозорість та об’єктивні критерії при прийнятті рішень.

Як і А. Приходько, песимістичні прогнози дає Ю. Хамига: «упровадження електронної системи закупівель Prozorro не сприяло подоланню наявних проблем у досліджуваній сфері» (Хамига, 2020, с. 118). Як зазначає Ю. Хамига, у сфері державних закупівель зберігається низка актуальних проблем, серед яких – штучне звуження або навмисно нечітке формулювання предмета закупівлі, використання формальних підстав для дискваліфікації переможців, ризик змови між постачальниками, а також розподіл закупівлі на менші частини з метою обходу вимог щодо проведення конкурентних торгів.

Загалом, ми солідарні із думкою (Трепак, 2020, с. 211-212) про те, що успішне застосування будь-яких аналітико-статистичних технологій у попередженні / протидії корупції в державі можливе лише за наступних умов:

1) абсолютне розділення приватного і суспільного (державного) інтересу – має стати принциповою та безумовною вимогою до службових осіб органів публічної влади;

2) на загальносуспільному рівні слід визнати за кожною службовою особою її невід'ємне право на наявність особистих, приватних інтересів; необхідно відмовитися від наївного та нереалістичного пошуку кандидатів на посади, що таких інтересів не мають;

3) потрібно узгодити умовний перелік приватних інтересів службової особи, прагнення до досягнення яких є природнім та не полягає у зловживанні владними повноваженнями. До таких треба впевнено віднести такі інтереси: отримання високої заробітної плати та інших офіційних засобів фінансового та матеріального характеру; просування по службі (кар'єрні амбіції, професійна самореалізація); високий соціальний статус; можливість мати власну справу, зайняття якою вимагатиме дотримання додаткових обмежень та суворого контролю з боку держави.

Тобто, змінити ситуацію неможливо без вираження політичної волі вищого рівня. Усі інші заходи, запропоновані для попередження / протидії політичній корупції як превентивного, так репресивного характеру, без цієї політичної волі не будуть ефективними.

Згідно з висновками Г. Блінової (Блінова, 2019, с. 396-398), запровадження аналітико-статистичних систем для моніторингу та запобігання корупції в органах державної влади може бути результативним лише за умови системного підходу до цифрової трансформації публічного управління. Насамперед, йдеться про необхідність розробки концепції цифрової держави, яка передбачає створення електронної публічної адміністрації, цифрового робочого місця для держслужбовців, а також механізмів моніторингу ефективності діяльності органів влади. Ці заходи мають бути підкріплені галузевими інформаційними стратегіями та стандартизованими підходами до роботи з цифровими інструментами.

Не менш важливими є упорядкування нормативно-правового поля у сфері інформаційного забезпечення та уніфікація термінології, що використовується у цій галузі. Окремо підкреслюється необхідність запровадження постійного контролю за інформаційним обміном між структурами публічної адміністрації з метою виявлення неефективних або штучно ускладнених процедур. Водночас необхідно чітко регламентувати статус і повноваження відповідних інформаційних підрозділів, а також забезпечити дієвий механізм дисциплінарної відповідальності за порушення в цій сфері.

Для досягнення відчутного ефекту в боротьбі з корупцією важливо забезпечити високий рівень інформаційної безпеки, подолати цифрову нерівність між центральними та місцевими органами влади, а також залучити громадян до активної участі в управлінських процесах. Це потребує єдиних стандартів ідентифікації осіб, уніфікованих підходів до створення та обробки електронних даних, а також безперебійного функціонування державних інформаційних систем незалежно від технічної бази.

Таким чином, можна констатувати наступне.

По-перше, цифровізація не є панацеєю, здатною автоматично вирішити проблему корупції в державі. Навпаки, цифрові технології, якщо вони впроваджуються без належної концептуальної підготовки, можуть призвести до появи нових форм електронної бюрократії чи навіть електронної корупції. Це

означає, що будь-яка антикорупційна політика, заснована на цифрових технологіях, має спиратися на чітко визначені правові принципи, враховувати можливі ризики та запобігати перетворенню технократичних рішень на інструменти тиску чи зловживання владою.

По-друге, цифрові технології набувають реальної ефективності лише за умови комплексного впровадження. Наприклад, впровадження тих або інших системи антиплагіату в системі закладів вищої освіти буде ефективним лише у поєднанні з відкритим доступом до студентських робіт дозволяє значно знизити рівень побутової корупції. Це означає, що технологічні інновації мають працювати не ізольовано, а вбудовуватися у ширшу систему публічного контролю, прозорості та підзвітності. Тобто, в Україні під час впровадження цифрових антикорупційних інструментів варто передбачати їх інтеграцію з іншими управлінськими та соціальними механізмами, щоб мінімізувати ризик того, що окремі рішення стануть лише символічними або легко обхідними.

По-третє, необхідно враховувати соціальні і культурні обмеження. Як показує досвід інших країн, інструменти, запозичені з західних моделей, можуть бути неефективними, якщо вони не адаптовані до національного контексту. Для України це означає, що цифрові інструменти повинні розроблятися з урахуванням місцевих реалій, включаючи рівень цифрової грамотності населення, ступінь довіри до держави, соціально-економічні умови регіонів.

По-четверте, технологічні інновації, з одного боку, підвищують прозорість, але з іншого – створюють нові вразливості. Наприклад, оператори інформаційних систем можуть самі стати джерелами витоків даних чи маніпуляцій. Це підкреслює необхідність проведення регулярних антикорупційних експертиз не лише адміністративних процедур, а й самих програмних рішень, щоб унеможливити технічні «лазівки» для зловживань. У практичній площині це означає, що українським розробникам і замовникам цифрових антикорупційних рішень потрібно одразу закладати механізми захисту даних, аудиту безпеки та внутрішнього контролю.

Нарешті, п’ятий момент полягає у важливості концептуального планування цифрових антикорупційних стратегій. Розробка окремих проектів без єдиної загальної концепції лише створює розрізнені ініціативи, що не матимуть системного впливу. Потрібне чітке бачення перспектив, ризиків, етапів впровадження, а також розуміння меж застосування цифрових технологій. Для України це означає потребу у формуванні національної стратегії цифрового антикорупційного управління, яка б не тільки передбачала технічне впровадження рішень, а й інтегрувала їх у ширший контекст правової політики, з урахуванням соціальних, економічних та культурних чинників. Тільки така комплексна стратегія дозволить уникнути небезпеки перетворення антикорупційних цифрових інструментів на формальні або навіть репресивні механізми.

З огляду на нерівномірність інституційного розвитку, неоднозначність політичної волі та фрагментарність цифрової трансформації державного управління в Україні, доцільним є формування сценарного аналізу подальшого розвитку цифрової антикорупційної інфраструктури. Такий підхід дозволяє врахувати як наявні тенденції, так і потенційні обмеження реалізації технологічного потенціалу у сфері запобігання корупції. Модель трьох сценаріїв – песимістичного, реалістичного та оптимістичного – окреслює межі можливого й служить інструментом аналітичної оцінки стратегічних умов, за яких цифрові інструменти можуть перетворитися з допоміжного засобу на системний чинник інституційної доброчесності.

1. У межах песимістичного сценарію цифрова трансформація антикорупційної політики зберігає суто декоративну функцію. Технологічні інструменти – системи відкритих даних, автоматизовані аудити, модулі ризик-аналізу – залишаються формально впровадженими, проте не інтегруються у реальні механізми прийняття рішень. Ключові інститути або не мають повноважень для дій на основі аналітичних даних, або свідомо ігнорують сигнали цифрових систем. У таких умовах цифрові інструменти використовуються для легітимації чинного порядку, а не для його трансформації.

Головним ризиком цього сценарію є посилення суспільного цинізму та втрата довіри до цифрових реформ як таких.

Додатковим чинником цього сценарію є поступова інерція системи: інституційна та політична культура чинить пасивний спротив змінам, адаптуючи навіть найсучасніші рішення під логіку «старої гри». У такій конфігурації автоматизація процедур перетворюється на спосіб формалізації бездіяльності: наприклад, публікація даних не супроводжується їх аналізом; аналітичні висновки не мають нормативної сили; порушення фіксуються, але не тягнуть за собою санкцій. Така цифровізація не лише не знижує рівень корупції, а й створює новий рівень імітації доброчесності, технологічно оформлений, але політично порожній.

2. У межах реалістичного сценарію впровадження цифрових антикорупційних технологій продовжується, проте зберігає фрагментарний характер. Деякі державні інституції, особливо ті, що мають зовнішню підтримку (наприклад, у межах співпраці з міжнародними партнерами), поступово інтегрують аналітичні інструменти у свою роботу. Успішними є проєкти, де технології мають чітку інституційну прив’язку, політичне покриття та наявні компетентні команди. Проте загальна система залишається гетерогенною: частина органів працює з цифровими інструментами, інші – ігнорують або симулюють їх використання. Такий сценарій відповідає складній реальності публічного управління в Україні, де прогрес завжди має точковий характер.

У цьому варіанті ймовірне поступове формування «осередків цифрової доброчесності», які задаватимуть стандарт для інших. Динаміка цього процесу залежатиме від кількох факторів: політичної волі на вищому рівні, тиску громадськості, конкурентної боротьби між інституціями, а також можливості технологій реально покращувати управління. Такий сценарій не передбачає радикального перелому, але дозволяє говорити про поступове укорінення цифрових рішень у повсякденну практику публічного управління, із перспективою масштабування найуспішніших кейсів.

3. У межах оптимістичного сценарію цифрова антикорупційна інфраструктура стає системоутворювальним елементом публічного управління. Технологічні рішення – від алгоритмічного моніторингу до систем прогнозування – інтегруються у ключові процеси державної служби, бюджетного нагляду, державних закупівель, електорального адміністрування. Це супроводжується зміною управлінської культури: ухвалення рішень дедалі більше базується на даних, а не на політичній доцільності; керівники несуть відповідальність за ігнорування аналітичних сигналів; цифрові інструменти перестають бути новацією і стають адміністративною нормою.

За таких умов технології не лише виявляють порушення, а й формують передумови для запобігання: рання діагностика, прогнозування ризиків, персоналізовані моделі поведінки чиновників або учасників ринку. Інституції не бояться делегувати частину функцій автоматизованим системам, бо мають довіру до алгоритмів. Відкритість даних забезпечується не формально, а вбудовується у логіку підзвітності. У результаті цифрова антикорупційна екосистема починає виконувати не лише контрольну, а й трансформаційну функцію, змінюючи спосіб взаємодії між державою і громадянами.

Отже, сам по собі розвиток інформаційних технологій, навіть найсучасніших, не гарантує автоматичного скорочення корупційних практик, якщо він не підкріплений політичною волею, культурними змінами та наявністю ефективних інституцій. Більш того, певні технологічні рішення, такі як блокчейн або криптовалютні транзакції, можуть не зменшувати, а навіть створювати нові можливості для зловживань, особливо якщо урядові структури не мають належних технічних і правових механізмів контролю за ними.

Сучасні цифрові інструменти часто функціонують у соціальному середовищі, де існують ризики маніпуляцій, астротурфінгу, замовних публікацій та створення хибної громадської думки. Без належного порівняння даних із незалежних джерел будь-які аналітико-статистичні системи, що аналізують публікації ЗМІ чи соціальних мереж, ризикують потрапити у пастку дезінформації. Тут стає очевидною важливість не лише технічних рішень, а й

нормативної основи, яка забезпечує захист викривачів корупції, рівність сторін перед законом і обов'язковість державної реакції на виявлені порушення. Саме в цьому розрізі український досвід показує: без належної правової та політичної основи навіть найбільш досконалі технології можуть залишитися формальними або навіть шкідливими.

Додаткову складність становлять ризики, пов'язані з безпекою обробки даних, включаючи можливість несанкціонованого доступу, витоків, або зловживань з боку операторів систем. Тому цифровізація повинна супроводжуватися чітким планом аудиту, перевірки алгоритмів, забезпечення безпеки програмних рішень та постійним оновленням стандартів відповідно до міжнародних вимог. Без цих заходів навіть найкращі інновації перетворюються на формальні символи боротьби з корупцією, що не мають реальної сили. Саме тому для України важливо інтегрувати впровадження цифрових рішень у ширший національний контекст: враховувати соціокультурні особливості, розриви цифрової грамотності між регіонами, а також необхідність громадського контролю адміністраторів державних інформаційних систем.

Нарешті, особливий акцент робиться на потребі розробки національної стратегії цифрового антикорупційного управління. Розрізнені ініціативи, що діють без координації, не формують системного ефекту, а іноді навіть посилюють нерівність чи бюрократичні перепони. Комплексний підхід, що враховує правові, технологічні, економічні й соціальні аспекти, здатний забезпечити стійке вбудування цифрових рішень у державне управління.

Запропонована сценарна модель дозволяють окреслити межі можливого розвитку цифрових антикорупційних інструментів в Україні з урахуванням внутрішніх політичних, інституційних і культурних обмежень. Вона демонструє, що технології не є самодостатнім чинником змін, а лише віддзеркалюють рівень готовності політичної системи до оновлення. Лише за умов реального перетворення аналітичних платформ із формального декору на дієвий механізм контролю та відповідальності можливий перехід від фрагментарної цифровізації до комплексної інституційної доброчесності. Лише так можна уникнути

сценарію, коли цифрові інструменти стають новою формою тиску, а не реальним засобом прозорості й підзвітності. Технології – це лише інструмент, а справжня антикорупційна ефективність народжується на перетині політичної волі, ефективного управління та свідомої участі громадянського суспільства.

Висновки до третього розділу

Таким чином, узагальнюючи висновки третього розділу, можна зазначити наступе:

По-перше, сучасні аналітико-статистичні технології є ключовим елементом у побудові антикорупційної інфраструктури держави. Вони охоплюють широкий спектр рішень: від базових інформаційних технологій збору та обробки даних до складних систем підтримки прийняття рішень, що поєднують математичне моделювання, візуалізацію та аналітичну інтерпретацію. Головна перевага таких систем полягає в зменшенні людського фактору, автоматизації рутинних завдань і підвищенні точності виявлення аномалій та відхилень. Це дозволяє державі не лише знижувати ризики навмисних спотворень, а й оптимізувати ресурси внутрішнього і зовнішнього контролю.

Окреме місце займає розвиток корпоративних і бізнес-аналітичних систем, що інтегрують у собі облік, планування, управління логістикою, клієнтами, матеріальними потоками та кадрами. Їх роль у попередженні / протидії корупції важлива насамперед тим, що вони створюють середовище прозорої взаємодії між різними структурними підрозділами, забезпечуючи аналітичну підтримку для всіх рівнів управління. Найсучаснішим напрямом є впровадження генеративного штучного інтелекту, здатного не лише аналізувати, а й створювати нові дані, генерувати гіпотези, моделювати сценарії, тим самим виводячи антикорупційну аналітику на рівень стратегічного прогнозування.

Тому сучасні аналітико-статистичні системи вже не можна розглядати як допоміжний інструмент – вони стають основою для побудови сучасного державного управління. Їх впровадження вимагає не лише фінансових інвестицій, а й розвитку аналітичної культури в державі, адже ефективність

цифрових рішень завжди залежить від того, наскільки користувачі – як на рівні держави, так і на рівні бізнесу – здатні інтегрувати їх у щоденні управлінські процеси. Це формує новий стандарт прозорості та підзвітності, без якого боротьба з корупцією в XXI столітті стає неможливою.

Антикорупційні стратегії з використанням інноваційних технологій формуються через два ключові напрями: інституційно-державний (зверху вниз) та громадянсько-суспільний (знизу вгору). Перший напрям забезпечує нормативне підґрунтя та контроль, створюючи юридичну рамку для впровадження цифрових рішень, тоді як другий активізує участь громадськості, залучаючи активістів, журналістів, дослідників до моніторингу державних практик. Лише синергія цих двох підходів дозволяє будувати стійку систему, де технологічні інновації стають інструментом не лише для контролю за громадянами, а й для контролю над владою.

Аналіз сучасних практик показує, що в арсеналі цифрових антикорупційних технологій існує чотири великі блоки: методологічні розробки, аналіз вторинних даних, автоматизовані системи аналізу текстових даних та експериментальні проекти на основі машинного навчання й штучного інтелекту. Кожен із них дає різні результати, але лише у комплексі вони створюють повноцінну картину – від виявлення патернів і аномалій до формування доказової бази для судових чи управлінських рішень. При цьому експериментальні розробки є особливо цінними, оскільки демонструють, як можна поєднати теоретичні моделі з реальними кейсами для отримання конкретних результатів.

Цифровізація сама по собі не гарантує ефективної боротьби з корупцією, а іноді навіть створює нові ризики – від електронної бюрократії до маніпуляцій із даними чи технологіями. Тому важливо не лише впроваджувати окремі технічні рішення, а й будувати навколо них стратегію, що враховує соціальні, правові й культурні фактори. Без наявності політичної волі будь-які інструменти залишаються формальними, а системні зміни є неможливими. Це стосується як

внутрішньої архітектури управління, так і зовнішнього контролю за публічною владою.

Важливо підкреслити й те, що сама структура ризиків, пов’язаних з цифровізацією, є набагато складнішою, ніж може здаватися на перший погляд. Вона охоплює не лише хакерські атаки, а й внутрішні витоки, зловживання операторами систем, а також ризики, пов’язані з монополізацією даних та контролем над їх використанням. Цифрові технології вимагають постійного аудиту, правового регулювання, прозорого розподілу компетенцій та впровадження механізмів публічного контролю. Лише за таких умов можна уникнути сценарію, коли інновації стають ще одним каналом для корупційних практик.

Тому ефективне попередження / протидія корупції в державі потребує розробки національної стратегії цифрового антикорупційного управління, яка об’єднує технічні, правові й управлінські компоненти в єдину систему. Без такої стратегії всі ініціативи залишатимуться розрізненими, локальними і не матимуть системного впливу. Тільки цілісний підхід дозволяє поєднати ефективність технологій із довірою суспільства, прозорістю влади та стійкістю до нових викликів цифрової доби.

ВИСНОВКИ

Дисертаційне дослідження є комплексним аналізом ролі інноваційних аналітико-статистичних технологій попередження корупції в сучасній державі, що дозволило досягти комплексних результатів, які можуть бути викладені у таких положеннях:

1. З’ясовано сутнісні характеристики понять «попередження корупції» та «інноваційна аналітико-статистична технологія». Встановлено, що перше поняття охоплює не лише юридичні норми та інституційні процедури, а й цифрові, аналітичні, інформаційні практики, які формують інфраструктуру превентивного та реактивного впливу на корупційні загрози. Визначено, що інноваційна аналітико-статистична технологія в широкому значенні є сукупністю методів та інструментів, що базуються на використанні математичних та статистичних методів аналізу даних з метою виявлення корисних залежностей та закономірностей в даних, підвищення ефективності прийняття рішень та виявлення аномалій у різних сферах діяльності. У вузькому – це процес використання найсучасніших методів та технологій аналізу даних, таких як машинне навчання, глибинне навчання, нейронні мережі, обробка природної мови, аналіз графів тощо з метою виявлення складних залежностей та корисних закономірностей в даних. До таких технологій відносяться також методи аналізу даних у режимі реального часу, які дозволяють отримувати швидкі та точні результати аналізу великих обсягів даних.

2. Проаналізовано стан наукової розробки проблеми інноваційних аналітико-статистичних технологій попередження корупції. Виявлено, що в українському контексті превалює нормативно-правовий і організаційно-інституційний підхід, тоді як методи цифрової діагностики, виявлення аномалій, використання машинного навчання та поведінкового моделювання залишаються недостатньо розвиненими. Робота заповнює цю прогалину, пропонуючи міждисциплінарну рамку з урахуванням досягнень соціальної кібернетики, аналітики даних та публічної політики.

3. Обґрунтовано методологічну рамку дослідження, що базується на поєднанні загальнонаукових принципів (об’єктивності, наукової обґрунтованості, історизму, комплексності, всебічності) та низки підходів (інституційного, системного, нормативного, структурно-функціонального, поведінкового, емпіричного, прогностичного). Таке поєднання дало змогу охопити як макрорівень (державна політика, правові системи), так і мікрорівень (поведінка користувачів, структура алгоритмів, практики ухвалення рішень).

4. Розкрито роль держави як середовища не лише виникнення, а й попередження / протидії корупції. Встановлено, що корупція є інституційним результатом збою в механізмах публічного контролю, розподілу повноважень і легітимації політичного впливу. Ефективна антикорупційна політика потребує не просто формального посилення інститутів, а зміни логіки їх функціонування на основі відкритості, цифрової підзвітності й громадського моніторингу. Саме ці функції можуть бути делеговані аналітичним цифровим системам.

5. Систематизовано типи та функції аналітико-статистичних технологій. У межах дослідження запропоновано класифікацію за функціональними ознаками: технології збору даних, їхньої структуризації, системи візуалізації, моніторингу, DSS-модулі ухвалення рішень та системи прогнозного аналізу. Показано, що ефективність таких технологій залежить від рівня їх інституційної інтеграції, прозорості алгоритмів, доступності для зовнішнього аудиту та здатності до самонавчання.

6. Охарактеризовано аналітико-статистичні підходи до виявлення корупційних загроз. Ключовою новацією є моделі аналізу поведінкових шаблонів посадовців, виявлення інсайдерських дій у системах доступу до даних, аналіз аномалій у публічних закупівлях, бюджетному плануванні й адмініструванні. Підкреслено роль алгоритмів попередження ризиків, а не лише фіксації наслідків порушень, що дозволяє перейти від реактивної до превентивної логіки антикорупційного управління.

7. Досліджено технологічні платформи, на яких ґрунтується антикорупційна аналітика. Вони охоплюють широкий спектр рішень: від базових

інформаційних технологій збору та обробки даних до складних систем підтримки прийняття рішень, що поєднують математичне моделювання, візуалізацію та аналітичну інтерпретацію. Головна перевага таких систем полягає в зменшенні людського фактору, автоматизації рутинних завдань і підвищенні точності виявлення аномалій та відхилень.

8. Антикорупційні стратегії з використанням інноваційних технологій формуються через два ключові напрями: інституційно-державний (зверху вниз) та громадянсько-суспільний (знизу вгору). Перший напрям забезпечує нормативне підґрунтя та контроль, створюючи юридичну рамку для впровадження цифрових рішень, тоді як другий активізує участь громадськості, залучаючи активістів, журналістів, дослідників до моніторингу державних практик. Аналіз сучасних практик показує, що в арсеналі цифрових антикорупційних технологій існує чотири великі блоки: методологічні розробки, аналіз вторинних даних, автоматизовані системи аналізу текстових даних та експериментальні проекти на основі машинного навчання й штучного інтелекту. Кожен із них дає різні результати, але лише у комплексі вони створюють повноцінну картину – від виявлення патернів і аномалій до формування доказової бази для судових чи управлінських рішень.

9. Сформульовано практичні рекомендації щодо розробки та реалізації національної стратегії цифрового антикорупційного управління. Запропоновано принципи: інтеграція відкритих даних, автоматизація оцінки ризиків, алгоритмічний аудит, правове регулювання доступу до державних даних, підтримка цифрової грамотності службовців, участь громадськості в тестуванні систем. Здійснено сценарне моделювання розвитку цифрової антикорупційної інфраструктури в Україні. Виокремлено песимістичний сценарій (цифровізація як симуляція), реалістичний (часткове впровадження із закріпленням «острівців доброчесності») та оптимістичний (технології як системоутворюючий інструмент публічного управління). Обґрунтовано, що політична воля, нормативна адаптація та розвиток цифрової культури в управлінні є ключовими умовами переходу до сприятливого сценарію.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

Автоматизація виробничого підприємства : Системи управління виробництвом. *Expresssoft.com.ua*. URL: https://expresssoft.com.ua/uk/avtomatizacija-2/upravlinnja-virobnictvom/ (дата звернення: 14.02.2025).

Бабарикіна, Н. А. (2025). Інформаційні технології в сучасній державі: між регулюванням і цифровим закріпаченням. *Науково-теоретичний альманах Грані, 28*(1), 182-191. URL: https://doi.org/10.15421/172523 (дата звернення: 14.02.2025).

Басанцов, І. В., & Зубарева, О. О. (2016). *Корупція в Україні: сучасні реалії та ефективні засоби протидії : монографія*. Суми: Сумський державний університет.

Блінова, Г. О. (2019). *Адміністративно-правові засади інформаційного забезпечення органів публічної адміністрації в Україні: актуальні питання теорії та практики.* (Дисертація на здобуття ступеня доктора юридичних наук : 12.00.07 дисертація), Запорізький національний університет, Запоріжжя.

Болотіна, Є. В., Стешенко, Н. Л., & Бородай, А. В. (2023). Інституційний метод аналізу політичної системи. *Регіональні студії, 32*, 41–46. URL: http://regionalstudies.uzhnu.uz.ua/archive/32/6.pdf (дата звернення: 14.02.2025).

Бутенко, Т. А., & Сирий, В. М. (2020). *Інформаційні системи та технології : навчальний посібник*. Харків: ХНАУ імені В.В. Докучаєва. URL: https://repo.btu.kharkov.ua/bitstream/123456789/4849/1/INFO_SYSTEMS_20.pdf (дата звернення: 14.02.2025).

Бутченко, Т. І. (2004). *Еволюціÿ договірно концепці походження держави: соціально-філософський аналіз. Дисертація на здобуття наук. ступеню канд. філ. наук. Запорізьк. держ. ун-тет.*,

В Украине снова открыт Реестр коррупционеров. (2023). *Opendatabot.ua*. URL: https://opendatabot.ua/ru/analytics/corrupted-officials (дата звернення: 14.02.2025).

Валлє, В. (2015). *Корупція: роздуми після Майдану*. Київ: Дух і Літера.

Валюшко, І. В. (2013). Антикорупційна політика: концептуальні підходи. *Стратегічні пріоритети, 4*(29), 101-105.

Великий тлумачний словник сучасної української мови. (2007). (за ред. В. Т. Бусел). Київ; Ірпінь: ВТФ «Перун».

Віннічук, Ю., & Головньов, С. (2018). Як обманути систему держзакупівель на ProZorro. *Бізнес цензор*. URL: https://biz.censor.net.ua/resonance/3086528/yak_obmanuti_sistemu_derjzakupvel_na_prozorro (дата звернення: 14.02.2025).

Волошин, В. В. (2013). Принцип об’єктивності у соціально-гуманітарному пізнанні: фокус на релігієзнавстві. *Наука. Релігія. Суспільство, 3*, 29–34.

Всемирный обзор экономических преступлений. (2011). URL: http://www.pwc.com/en_UA/ua/services/forensic/assets/gecs_2011_report_ukraine_rus.pdf (дата звернення: 14.02.2025).

Гаращук, В. М. (1997). *Стратегія і тактика боротьби з корупцією. Концепція боротьби з корупцією в Україні. Міністерство юстиції України : підготовчі матеріали*. Київ: Координатор-центр правової реформи і законопроектних робіт при Міністерстві юстиції України.

Глазунов, В. В. (2012). *Українська олігархія в контексті сучасних трансформаційних процесів.* (Дисертація на здобуття ступеня доктора філософських наук : 09.00.03 – Соціальна філософія і філософія історії), Класичний приватний університет, Запоріжжя.

Гутуров, О. І. (2019). *Стратегічна інноватика : навчальний посібник*. Харків: ХНАУ.

Дедекаев, В. (1998). Тіньова економіка – шлях у нікуди. *Міліцейський кур’єр, 36*, 42-45.

Державний веб-портал бюджету для громадян. *Openbudget.gov.ua*. URL: https://openbudget.gov.ua/ (дата звернення: 14.02.2025).

Долбнєва, Д. В. (2019). Шляхи трансформації системи боротьби з економічними злочинами в Україні з урахуванням досвіду країн Європейського Союзу. *ScienceRise. Серія «Економічні науки», 2-3*(55-56), 21-27. URL: https://doi.org/10.15587/2313-8416.2019.163108 (дата звернення: 14.02.2025).

Європейський кодекс поліцейської етики. Рекомендація (2001) 10 Комітету Міністрів Ради Європи від 19 вересня 2001. (2001). URL: https://hrea.org/wp-content/uploads/2021/02/Recommendation-Rec200110_European-Code-of-Police-Ethics_Ukrainian.pdf (дата звернення: 14.02.2025).

єДокумент – новий тимчасовий цифровий документ на період воєнного стану. (2022). *ДІЯ*. URL: https://diia.gov.ua/news/yedokument-novij-timchasovij-cifrovij-dokument-na-period-voyennogo-stanu (дата звернення: 14.02.2025).

Задорожний, С. А. (2016). *Механізми запобігання та протидії корупції в органах місцевої влади.* (Дисертація на здобуття ступеня кандидата наук з державного управління : 25.00.02 – Механізми державного управління дисертація), Національна академія державного управління при Президентові України, Київ.

Захарова, І. В., & Філіпова, Л. Я. (2013). *Основи інформаційно-аналітичної діяльності : навчальний посібник*. Київ: Центр учбової літератури.

Карпенко, М. І., & Пашковський, В. В. (2013). Сучасні ознаки корупційної злочинності та їх зміст. *Юридична наука, 5*, 54-61. URL: http://nbuv.gov.ua/UJRN/jnn_2013_5_8 (дата звернення: 14.02.2025).

Кивлюк, О., Гарбар, Г., Пунченко, О., Арабаджиєв, Д., & Андрюкайтене, Р. (2024). Філософія сталого розвитку в умовах цифрової трансформації як основа збалансованого зростання, соціального добробуту та екологічної стійкості. *Humanities Studies, 21*(98), 45-54. URL: https://doi.org/10.32782/hst-2024-21-98-06 (дата звернення: 14.02.2025).

Кікалішвілі, М. В. (2021). *Теоретико-прикладні засади формування та реалізації стратегії й тактики протидії корупційній злочинності.* (Дисертація на здобуття ступеня доктора юридичних наук : 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право), Університет митної служби та фінансів; Дніпропетровський державний університет внутрішніх справ, Дніпро.

Кіндратець, О. М. (2022). *Електронні петиції та їх значення в формуванні е-демократії.* Paper presented at the Імідж і репутація: сучасні тенденції і виклики. Міжнар. наук.-практ. конф., Київ, 23 вересня. 2022 р. / М-во освіти і науки України, Київ. нац. ун-т культури і мистецтв, Київ. URL: https://kzgizh.knukim.edu.ua/images/nauka/konferentsii/2022-zbirnyk-imidzh-i-reputatsiia.pdf (дата звернення: 14.02.2025).

Климко, Т. Ю., & Мельник, О. О. (2015). Корпоративне шахрайство: реалії сучасності. *Науковий вісник Ужгородського університету. Серія «Економіка», 2*(46), 185-190.

Ковтун, Н. (2011). Методи індикативної оцінки можливого шахрайства у фінансовій сфері. *Вісник Київського національного університету імені Тараса Шевченка. Серія «Економіка», 123*, 11-15.

Конвенція Організації Об'єднаних Націй проти корупції від 31.10.2003 р. (2003). URL: https://www.un.org/ru/documents/decl_conv/conventions/corruption.shtml (дата звернення: 14.02.2025).

Копча, В. В. (2020). Сучасна держава: основні підходи до розуміння. *Науковий вісник Міжнародного гуманітарного університету. Серія Юриспруденція, 43*, 13-17. URL: https://doi.org/10.32841/2307-1745.2020.43.3 (дата звернення: 14.02.2025).

Костенко, Д. В. (2020). *Система запобігання корупції в Україні: становлення та розвиток.* (Дисертація на здобуття ступеня кандидата наук з державного управління : 25.00.01 – Теорія та історія державного управління дисертація), Інститут підготовки кадрів Державної служби зайнятості України Міністерства соціальної політики України, Київ.

Костенко, О. М. (2008). Корупція кризового типу: поняття і шляхи протидії. *Боротьба з організованою злочинністю і корупцією (теорія і практика), 18*, 136-141. URL: http://nbuv.gov.ua/UJRN/boz_2008_18_15 (дата звернення: 14.02.2025).

Костенко, О. М. (2016). Яким «каменем» зневажили «будівничі» вітчизняної антикорупційної політики? *Віче, 3-4*, 12-13.

Кохан, Г. В. (2013). *Явище політичної корупції: теоретико-методологічний аналіз : монографія*. Київ: НІСД. URL: https://irbis-nbuv.gov.ua/ulib/item/ukr0000018972 (дата звернення: 14.02.2025).

Крохмаль, Н. (2004). *Історичні форми саморегуляції соціального процесу*. Запоріжжя: Просвіта.

Кудінов, І. О., & Яцина, Ю. О. (2020). Чи можливо ідентифікувати корупційні схеми під час виборів? *Center for Independent Social Research*. URL: https://cisr.zp.ua/publications/election-corruption-detection.html (дата звернення: 14.02.2025).

Кудінов, І. О., & Яцина, Ю. О. (2024). Інноваційні технології автоматизації збору та обробки даних у дослідженнях політичних процесів та ситуацій. In *Технології державотворення в умовах сучасної політичної дійсності : колективна монографія / за заг. ред. Н. В. Горло* (С. 267-288). Запоріжжя: Запорізький національний університет. URL: https://dspace.znu.edu.ua/jspui/bitstream/12345/25198/1/0060900.pdf (дата звернення: 14.02.2025).

Кудінов, І. О., & Яцина, Ю. О. (2025). Статистичні методи пошуку шахрайства під час виборів : огляд останніх досліджень. *Center for Independent Social Research*. URL: https://cisr.zp.ua/publications/election-fraud.html (дата звернення: 14.02.2025).

Куц, Ю. О., Сінченко, В. М., Мамонова, В. В., & Газарян, С. В. (2011). *Територіальна громада: знанєвість, дієвість : монографія* (за ред. Ю. О. Куц). Харків: Віровець А.П. "Апостроф".

Кушнарьов, І. В. (2017). Політична корупція у країнах Балтії: успішний досвід на пострадянському просторі. *Держава і право. Серія "Політичні науки", 77*, 92-105.

Кушнарьов, І. В. (2018). *Політична корупція: порівняльно-політологічна концептуалізація : монографія*. Київ: Ін-т держави і права ім. В.М. Корецького НАН України; Видавництво «Юридична думка».

Лепський, М. А. (2012). Моделювання у стратегічному прогнозуванні політичних ситуацій та процесів. In *Стратегічне прогнозування політичних ситуацій та процесів : монографія / за заг. ред. М.А. Лепського* (pp. 459-488). Запоріжжя: ЗНУ.

Лепський, М. А. (2022). *Соціологія агресії : монографія*. Запоріжжя: КСК-Альянс.

Лісовий, В. С. (2001). Аналіз і синтез. *Енциклопедія Сучасної України / редкол. : І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ*. URL: https://esu.com.ua/article-44034

Лозинський, О. М. (2021). *Психологічні чинники інтолерантного ставлення громадян до корупції.* (Дисертація на здобуття ступеня кандидата психологічних наук : 19.00.05 - Соціальна психологія; психологія соціальної роботи), Інститут соціальної та політичної психології НАПН України, Київ.

Мазур, І. (2005). Корупція як інститут тіньової економіки. *Економіка і право, 8*, 34-38.

Марич, М. І. (2013). Поняття і сутність корупції та корупційної злочинності. *Держава і право. Юридичні і політичні науки, 61*, 310-317. URL: http://nbuv.gov.ua/UJRN/dip_2013_61_50.

Мельник, М. І. (2001). *Корупція: сутність, поняття, заходи протидії: монографія*. Київ: Атіка.

Мельник, М. І. (2004). *Корупція – корозія влади (соціальна сутність, тенденції та наслідки, заходи протидії) : монографія*. Київ: Юридична думка.

Мельник, М. І., & Хавронюк, М. І. (1998). Правові та організаційні заходи протидії корупції: зарубіжний досвід. *Науковий вісник Національної академії внутрішніх справ України, 4*, 119-134.

Методи вдосконалення технологічного процесу. (2022, 04.07.2022). *Український Тиждень*. URL: https://tyzhden.ua/metody-vdoskonalennia-tekhnolohichnoho-protsesu/ (дата звернення: 14.02.2025).

Методологія наукових досліджень : навчальний посібник для підготовки докторів філософії спеціальностей 161 Хімічні технологія та біоінженерія, 162 Біотехнології та біоінженерія, 163 Біомедична інженерія / уклад.: Астрелін І. М., Косогіна І. В., Кирій С. О. (2021). Київ: КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/server/api/core/bitstreams/889e6ada-9c5f-4404-837f-62c7171645e0/content (дата звернення: 14.02.2025).

Монастирський, Г. Л. (2014). *Теорія організації : підручник*. Тернопіль: ТНЕУ.

Музика, І. В. (2012). Принцип історизму у царині досліджень вітчизняної соціології права кінця XIX – початку XX століття. *Альманах права, 3*, 239–243.

Наполеоновские планы | Цифровая ЗеУкраина: план развития digital-экономики. (2019). *Liga.net.* URL: https://tech.liga.net/technology/article/ tsifrovaya-zeukraina-plan-razvitiya-digital-ekonomiki-dokument (дата звернення: 14.02.2025).

Невмережицький, Є. В. (2008). *Корупція в Україні: причини, наслідки, механізми протидії : монографія*. Київ: КНТ. URL: http://irbis-nbuv.gov.ua/cgi-bin/ua/elib.exe?Z21ID=&I21DBN=UKRLIB&P21DBN=UKRLIB&S21STN=1&S21REF=10&S21FMT=online_book&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=FF=&S21STR=ukr0001932 (дата звернення: 14.02.2025).

Нинюк, М., & Нинюк, І. (2015). Корупція як фактор загрози національній безпеці та суспільному ладу України. *Історико-правовий часопис, 2*, 71-76.

Новий тлумачний словник української мови : в 4 томах. (2000). (за ред. В. Яременко & О. Сліпушко). Київ: Аконіт.

Новіков, О. В. (2020). *Публічно-правове забезпечення протидії корупції в умовах регіонального розвитку.* (Дисертація на здобуття ступеня кандидата юридичних наук : 12.00.07 - Адміністративне право і процес; фінансове право; інформаційне право дисертація), Науково-дослідний інститут публічного права; Дніпропетровський державний університет внутрішніх справ, Київ.

Окунєв, О. Й., Бойко, О. І., & Лукін, С. Ю. (2018). *Антикорупційний комплаєнс: посібник для програми з підготовки осіб, відповідальних за реалізацію антикорупційної програми*. Київ: Професійна асоціація корпоративного управління, Центр міжнародного приватного підприємництва (CIPE).

Олещук, П. М. (2019). *Новітні політичні технології інформаційного впливу.* (Дисертація на здобуття ступеня доктора політичних наук : 23.00.02 – Політичні інститути та процеси), Київський національний університет імені Тараса Шевченка, Київ.

Попередження. *Словник української мови : в 11 томах*. URL: https://sum.in.ua/s/poperedzhennja (дата звернення: 14.02.2025).

Приходько, А. А. (2020). *Адміністративно-правове забезпечення запобігання та протидії корупції в Україні за умов євроінтеграції.* (Дисертація на здобуття ступеня доктора юридичних наук : 12.00.07 - Адміністративне право і процес; фінансове право; інформаційне право), Науково-дослідний інститут публічного права, Дніпропетровський державний університет внутрішніх справ України, Київ.

Про запобігання корупції: Закон України від 14.10.2014 № 1700-VII. (2025). *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/1700-18 (дата звернення: 14.02.2025).

Про інноваційну діяльність : Закон України від 04.07.2002 №40-IV. (2023). *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/40-15 (дата звернення: 14.02.2025).

Про нас. (2023). *Міністерство цифрової трансформації України*. URL: https://thedigital.gov.ua/ministry (дата звернення: 14.02.2023).

Про хмарні послуги. Закон України від 17.02.2022 №2075-IX. (2022). *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2075-20 (дата звернення: 14.02.2025).

Расулев, А., & Исмоилов, Б. (2020). Организационно-правовые аспекты применения цифровых технологий в противодействии коррупции: зарубежный опыт правоприменительной практики. *Общество и инновации, 1*(2), 300-320. URL: https://doi.org/10.47689/2181-1415-vol1-iss2-pp300-320 (дата звернення: 14.02.2025).

Рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в закладах вищої освіти. (2025). *Міністерство цифрової трансформації України, с.* 56. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Vykorystannya_AI_u_vyshchyy_osviti.pdf (дата звернення: 25.05.2025).

Рикова, Н. В. (2020). Держава в системі корпоративних інтересів і відносин: особливості правових обмежень. *Право та державне управління, 2*, 34-41. URL: https://doi.org/10.32840/pdu.2020.2.5 (дата звернення: 14.02.2025).

Рогульський, С. С. (2005). *Адміністративно-правові заходи боротьби з корупцією в Україні.* (Автореферат дисертації на здобуття ступеня кандидата юридичних наук : 12.00.07 - Адміністративне право і процес; фінансове право; інформаційне право), Київ.

Роджерс, Е. М. (2009). *Дифузія інновацій* (В. Старк, Trans.). Київ: Видавничий дім "Києво-могилянська академія".

Росохата, А. С. (2012). Аналіз теоретичних основ наукового прогнозування на засадах маркетингу. *Маркетинг і менеджмент інновацій, 2*, 99–111.

Свириденко, В. (ред.) (2002) Філософський енциклопедичний словник / В. І. Шинкарук (гол. редкол.) та ін. Київ: Інститут філософії імені Григорія Сковороди НАН України ; Абрис.

Селюченко, Н. Є., Заяць, Р. Я., & Живко, М. О. (2010). Суть корупції та шляхи її подолання. *Науковий вісник Львівського державного університету внутрішніх справ, 1*, 64-72.

Скиба, М. В. (2014). Сутність та роль держави: інституціональний аспект. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 18 : Економіка і право, 24*, 24-30. URL: http://nbuv.gov.ua/UJRN/Nchnpu_018_2014_24_6 (дата звернення: 14.02.2025).

Смирний, М. Ф. (2018). *Основи наукових досліджень : конспект лекцій для студентів усіх форм навчання за спеціальністю 141 – Електроенергетика, електротехніка та електромеханіка*. Харків: ХНУМГ ім. О. М. Бекетова.

Стогова, О. В. (2016). Люстрація як передумова ефективної боротьби з корупцією. *Сучасне суспільство, 1*, 167-177.

Суббот, А., & Дем'янчук, Ю. (2017). Засоби протидії та запобігання корупції в умовах реформування законодавства. *Підприємництво, господарство і право*(6), 113-117.

Тараненко, О. П. (2014). Сучасні заходи запобігання корупції у сфері державних закупівель. *Державне управління: теорія та практика, 2*, 12-19. URL: http://nbuv.gov.ua/UJRN/Dutp_2014_2_4 (дата звернення: 14.02.2025).

Терещук, О. В. (2000). *Адміністративна відповідальність за корупційні правопорушення.* (Автореферат дисертації на здобуття ступеня кандидата юридичних наук: 12:00:07), Київський ін-т внутрішніх справ при Національній академії внутрішніх справ України, Одеса.

Терлюк, І. (2021). "Держава" і "державність": до проблеми теоретико-правового та історико-правового змісту понять в контексті українського (національного) державотворення. *Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки", 8*(29), 17-28. URL: https://doi.org/10.23939/law2021.29.017 (дата звернення: 14.02.2025).

Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та

корупції. (2018). (за ред. А. Г. Чубенко, М. В. Лошицький, Д. М. Павлов, С. С. Бичкова, & О. С. Юнін). Київ: Ваіте.

Тофтул, М. Г. (2011). Індукція і дедукція. *Енциклопедія Сучасної України* / редкол. : І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ. URL: https://esu.com.ua/article-13371 (дата звернення: 14.02.2025).

Трепак, В. М. (2020). *Теоретико-прикладні проблеми запобігання та протидії корупції в Україні.* (Дисертація на здобуття ступеня доктора юридичних наук : 12.00.08 - Кримінальне право та кримінологія; кримінально-виконавче право), Львівський національний університет імені Івана Франка, Київ.

Трофименко, К. В. (2020). Аналіз етимології поняття "корпорація". *Економіка та суспільство, 22*. URL: https://doi.org/10.32782/2524-0072/2020-22-20 (дата звернення: 14.02.2025).

Тучак, Р. М. (2006). Корупція як соціально-правове явище. *Актуальні проблеми державного управління: зб. наук. праць, 3*(30), 203-209.

Українці найбільше довіряють програмі «Держава у смартфоні» та цифровізації - опитування «Рейтинг». (2021, 20.05.2021). *Міністерство цифрової трансформації України.* URL: https://thedigital.gov.ua/news/ukraintsi-naybilshe-doviryayut-programi-derzhava-u-smartfoni-ta-tsifrovizatsii-opituvannya-reyting (дата звернення: 14.02.2025).

Фоміна, М. В., & Кузьмеко, В. В. (2013). Сутінсть, форми і класифікація корупційних відносин. *Економічний вісник університету, 21/1*, 182-186.

Хамига, Ю. Я. (2020). *Фінансове шахрайство: критерії ідентифікації та напрями мінімізації.* (Дисертація на здобуття ступеня доктора філософії : 072 - Фінанси, банківська справа та страхування дисертація), Західноукраїнський національний університет, Тернопіль.

Хорішко, Л. (2024). Політичне лідерство як суспільно-політичний ресурс інформаційного суспільства й інформаційного простору держави. *Наукові перспективи (Naukovì perspektivi), 2*(44), 599-607. URL:

https://doi.org/10.52058/2708-7530-2024-2(44)-599-607 (дата звернення: 14.02.2025).

Цифрові трансформації в Україні: чи відповідають вітчизняні інституційні умови зовнішнім викликам та європейському порядку денному? (2020). *Поліський фонд міжнародних та регіональних досліджень*. URL: http://old.eap-csf.org.ua/initsiativi-unp-2020-analitichniy-dokument-tsifrovi-transformatsiyi-v-ukrayini-chi-vidpovidayut-vitchiznyani-institutsiyni-umovi-zovnishnim-viklikam-ta-yevropeyskomu-poryadku-dennomu-poliskiy/ (дата звернення: 14.02.2025).

Цокур, Є. Г. (2017). Вибори у сучасному світі: збереження демократії чи прикриття її руйнації? *Політичне життя, 1-2*, 4-8. URL: https://journals.donnu.edu.ua/index.php/pl/article/download/3998/4030 (дата звернення: 14.02.2025).

Чайка, І., & Цокур, Є. (2024). Цифровізація виборів в Україні і світі: етичні виміри феномену. *Humanities studies: Collection of Scientific Papers / Ed. V. Voronkova. Zaporizhzhia : Publishing house "Helvetica", 20*(97), 140–147. URL: https://doi.org/10.32782/hst-2024-20-97-16 (дата звернення: 14.02.2025).

Чернєй, В. В. (2014). Правове та організаційне забезпечення протидії злочинам у сфері державних фінансів. *Науковий вісник Національної академії внутрішніх справ, 2*, 3-14.

Чорнуцький, С. П. (2011). Суть і методика виявлення фактів фінансового шахрайства. *Економіка та держава, 7*, 127-131.

Шаган, О. В. (2014). Система принципів нормотворчості. *Науково-інформаційний вісник Івано-Франківського університету права ім. Данила Галицького, 9*, 64–69.

Шаркова, В. (2020). Коррупционные проявления, сопровождающиеся должностными и служебными лицами. *Knowledge, Education, Law, Management, 3*(6), 190-194. URL: https://doi.org/10.51647/kelm.2020.6.3.37 (дата звернення: 14.02.2025).

Шаховська, Н. І. (2022). Шкловський Йосип Самуїлович. *Енциклопедія Сучасної України* / редкол. : І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ. URL: https://esu.com.ua/article-77811 (дата звернення: 14.02.2025).

Юрченко, О. М. (2013). Засоби інформаційного забезпечення протидії організованій злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика), 2*(30), 84-92.

Яцина, Ю. О., & Кудінов, І. О. (2021). Про високі статистичні технології. *Union of Social Engineers of Ukraine*. URL: https://useu.org.ua/library/high-statistics.html (дата звернення: 25.05.2025).

Яцина, Ю. О., & Кудінов, І. О. (2022). Пошук статистичних аномалій в Big Data. *Union of Social Engineers of Ukraine*. URL: https://useu.org.ua/library/anomaly-detection.html (дата звернення: 25.05.2025).

Abellera, R., & Bulusu, L. (2018). *Oracle Business Intelligence with Machine Learning*. New York, NY: Springer. URL: https://doi.org/10.1007/978-1-4842-3255-2 (дата звернення: 14.02.2025).

Adam, I., & Fazekas, M. (2018). Are Emerging Technologies Helping Win the Fight Against Corruption in Developing Countries? *Pathways for Prosperity Commission Background Paper Series*(21). URL: https://doi.org/10.13140/RG.2.2.17930.52162 (дата звернення: 14.02.2025).

Aggarwal, C. C. (2017). *Outlier Analysis*. Cham, Switzerland: Springer International Publishing AG. URL: https://doi.org/10.1007/978-3-319-47578-3 (дата звернення: 14.02.2025).

AI21 : Building the Future of Enterprise AI. *ai21.com*. URL: https://www.ai21.com/ (дата звернення: 14.02.2025).

Althebyan, Q., & Panda, B. (2007). *A Knowledge-Base Model for Insider Threat Prediction.* Paper presented at the 2007 IEEE SMC Information Assurance and Security Workshop, West Point, NY, USA.

Alvarez, M. R., Levin, I., & Li, Y. (2018). Fraud, Convenience, and e-voting: How Voting Experience Shapes Opinions About Voting Technology. *Journal of*

Information Technology & Politics, 15(2), 1-33. URL: https://doi.org/10.1080/19331681.2018.1460288 (дата звернення: 14.02.2025).

Antropic : AI research and products that put safety at the frontier. *Anthropic.com*. URL: https://www.anthropic.com/ (дата звернення: 14.02.2025).

The Apache Software Foundation. *Lucy.apache.org*. URL: https://lucy.apache.org (дата звернення: 14.02.2025).

Applied Informatics for Industry 4.0. (2023). (N. Siddique, M. Shamsul, J. Wall, & S. M. Kaiser Eds.). Boca Raton, FL: CRC Press. URL: https://doi.org/10.1201/9781003256069 (дата звернення: 14.02.2025).

ArangoDB: Powerful Search Included. *Arangodb.com*. URL: https://www.arangodb.com/full-text-search-engine/ (дата звернення: 14.02.2025).

AssemblyAI Documentation. *AssemblyAI.com*. URL: https://www.assemblyai.com/docs (дата звернення: 14.02.2025).

Awati, K., & Scriven, A. (2023). *Data Science and Analytics Strategy: An Emergent Design Approach*. Boca Raton, FL: CRC Press. URL: https://doi.org/10.1201/9781003260158 (дата звернення: 14.02.2025).

Azzalini, A., & Scarpa, B. (2012). *Data Analysis and Data Mining*. New York: Oxford University Press.

Baesens, B., Vlasselaer, V. V., & Verbeke, W. (2015). *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques : a Guide to Data Science for Fraud Detection* Hoboken, New Jersey: Wiley.

Bagenholm, A., Bauhr, M., Grimes, M., & Rothstein, B. (2021). Introduction: Quality of Government: Why-What-How. In A. Bagenholm, M. Bauhr, M. Grimes, & B. Rothstein (Eds.), *The Oxford Handbook of the Quality of Government*. New York, NY: Oxford University Press. URL: https://doi.org/10.1093/oxfordhb/9780198858218.001.0001 (дата звернення: 14.02.2025).

Bandyopadhyay, S. (2023). *Decision Support System: Tools and Techniques*. Boca Raton, FL: CRC Press. URL: https://doi.org/10.1201/9781003307655 (дата звернення: 14.02.2025).

Bartunov, O. (2018). *Do you need a Full-Text Search in PostgreSQL?* Paper presented at the PGConf.eu, Lisbon. URL: www.postgresql.eu/events/pgconfeu2018/sessions/session/2116/slides/137/pgconf.eu-2018-fts.pdf (дата звернення: 14.02.2025).

Bayar, Y. (2017). Greenfield and Brownfield Investments and Economic Growth: Evidence from Central and Eastern European Union Countries. *Naše Gospodarstvo / Our Economy, 63*(3), 19-26. URL: https://doi.org/10.1515/ngoe-2017-0015 (дата звернення: 14.02.2025).

Beber, B., & Scacco, A. (2012). What the Numbers Say: A Digit-Based Test for Election Fraud. *Political Analysis, 20*(2), 211-234. URL: https://doi.org/10.1093/pan/mps003 (дата звернення: 14.02.2025).

Berk, R. (2019). *Machine Learning Risk Assessments in Criminal Justice Settings*. Cham, Switzerland: Springer. URL: https://doi.org/10.1007/978-3-030-02272-3 (дата звернення: 14.02.2025).

Berru, Y. T., Batista, V. F. L., Torres-Carrión, P., & Jimenez, M. G. (2020). Artificial Intelligence Techniques to Detect and Prevent Corruption in Procurement: A Systematic Literature Review. *ICAT 2019, CCIS, 1194*, 254-268. URL: https://doi.org/10.1007/978-3-030-42520-3_21 (дата звернення: 14.02.2025).

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network Anomaly Detection: Methods, Systems and Tools. *IEEE Communications Surveys & Tutorials, 16*(1), 303-336. URL: https://doi.org/10.1109/surv.2013.052213.00046 (дата звернення: 14.02.2025).

Borysenko, V., & Borysenko, T. (2021). *Concept and method for development of corporate information system*. Paper presented at the Fifth International Scientific and Technical Conference "Computer and Information Systems and Technologies", Kharkiv. URL: https://doi.org/10.30837/csitic52021232894 (дата звернення: 14.02.2025).

Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., . . . Ducheneaut, N. (2012). *Proactive Insider Threat Detection through Graph Learning and Psychological Context*. Paper presented at the 2012 IEEE Symposium on Security and Privacy Workshops. URL: https://doi.org/10.1109/spw.2012.29 (дата звернення: 14.02.2025).

Breunig, M. M., Kriegel, H.-P., Ng, R. T., & Sander, J. (2000). LOF: Identifying Density-Based Local Outliers. *ACM SIGMOD Record, 29*(2), 93-104. URL: https://doi.org/10.1145/335191.335388 (дата звернення: 14.02.2025).

Cappelli, D., Moore, A., & Trzeciak, R. (2012). *How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Westford, Massachusetts: Pearson Education, Inc.

Cassell, M. (2021). *A guide to client risk segmentation to optimize the impact of HIV programming*. URL: https://www.fhi360.org/sites/default/files/media/documents/epic-client-segmentation-guide.pdf (дата звернення: 14.02.2025).

Chan, L., Hogaboam, L., & Cao, R. (2022). *Applied Artificial Intelligence in Business: Concepts and Cases*. Cham, Switzerland: Springer Nature Switzerland AG. URL: https://doi.org/10.1007/978-3-031-05740-3 (дата звернення: 14.02.2025).

Chatera, M., Borgib, A., Slamaa, M. T., Sfar-Gandouraa, K., & Landoulsi, M. I. (2022). Fuzzy Isolation Forest for Anomaly Detection. *Procedia Computer Science*(207), 916-925. URL: https://doi.org/10.1016/j.procs.2022.09.147 (дата звернення: 14.02.2025).

Chen, J., Zhang, J., Qian, R., Yuan, J., & Ren, Y. (2023). An Anomaly Detection Method for Wireless Sensor Networks Based on the Improved Isolation Forest. *Applied Sciences, 13*(2). URL: https://doi.org/10.3390/app13020702 (дата звернення: 14.02.2025).

Chen, Y., & Malin, B. (2011). Detection of Anomalous Insiders in Collaborative Environments via Relational Analysis of Access Logs. *Proceedings of the First ACM Conference on Data and Application Security and Privacy - CODASPY*

'11, 63-74. URL: https://doi.org/10.1145/1943513.1943524 (дата звернення: 14.02.2025).

Cios, K. J., Pedrycz, W., & Swiniarski, R. W. (1998). Data Mining and Knowledge Discovery. In *Data Mining Methods for Knowledge Discovery* (pp. 1-26). New York, NY: Springer. URL: https://doi.org/10.1007/978-1-4615-5589-6 (дата звернення: 14.02.2025).

Cohen, W. W. (2015). Enron Email Dataset. Retrieved from http://www.cs.cmu.edu/~enron/ (дата звернення: 14.02.2025).

Cohere : The all-in-one platform for private and secure AI. *Cohere.ai*. URL: https://cohere.ai (дата звернення: 14.02.2025).

CYBERscape. (2022). *Momentumcyber.com*. URL: https://momentumcyber.com/docs/CYBERscape_4.7.22.pdf (дата звернення: 14.02.2023).

Dahl, R. A. (1961). The Behavioral Approach in Political Science: Epitaph for a Monument to a Successful Protest. *The American Political Science Review, 55*(4), 763-772. URL: https://doi.org/10.2307/1952525 (дата звернення: 14.02.2025).

Das, S., Islam, M. R., Jayakodi, N. K., & Doppa, J. R. (2019). Active Anomaly Detection via Ensembles: Insights, Algorithms, and Interpretability. *Journal of Artificial Intelligence Research, 80*, 127-172. URL: http://dx.doi.org/10.48550/arXiv.1901.08930 (дата звернення: 14.02.2025).

Das, S., Wong, W.-K., Fern, A., Dietterich, T. G., & Siddiqui, M. A. (2017). *Incorporating Feedback into Tree-based Anomaly Detection.* Paper presented at the Proceedings of Halifax, Nova Scotia, Canada, August 14th, 2017 (KDD 2017Workshop on Interactive Data Exploration andAnalytics (IDEA'17)). URL: https://arxiv.org/pdf/1708.09441.pdf (дата звернення: 14.02.2025).

The Data-Driven Blockchain Ecosystem: Fundamentals, Applications, and Emerging Technologies. (2023). (A. Khang, S. Chowdhury, & S. Sharma Eds.): CRC Press. URL: https://doi.org/10.1201/9781003269281 (дата звернення: 14.02.2025).

Davenport, T. H., & Mittal, N. (2023). *All in on AI: How Smart Companies Win Big with Artificial Intelligence*. Boston, Massachusetts: Harvard Business Review Press.

de Francesco, F., & Trein, P. (2020). How Does Corruption Affect the Adoption of Lobby Registers? A Comparative Analysis. *Politics and Governance, 8*(2), 116-127. URL: https://doi.org/10.17645/pag.v8i2.2708 (дата звернення: 14.02.2025).

DeepMind : Build AI responsibly to benefit humanity. *Deepmind.google*. URL: https://deepmind.google/about/ (дата звернення: 14.02.2025).

Dietrich, S., & Winters, M. B. (2021). Foreign aid and quality of government. In A. Bagenholm, M. Bauhr, M. Grimes, & B. Rothstein (Eds.), *The Oxford Handbook of the Quality of Government* (pp. 449-471). New York, NY: Oxford University Press. URL: https://doi.org/10.1093/oxfordhb/9780198858218.001.0001 (дата звернення: 14.02.2025).

Dou, Y., Liu, Z., Sun, L., Deng, Y., Peng, H., & Yu, P. S. (2020). *Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters.* Paper presented at the Proceedings of the 29th ACM International Conference on Information & Knowledge Management.

Dozorro - громадський контроль держзакупівель. *Dozorro.org*. URL: https://dozorro.org/ (дата звернення: 14.02.2025).

Drahos, P., & Braithwaite, J. (2002). *Information feudalism*. London, UK: Earthscan Publications Ltd.

Drucker, P. F. (1984). *Innovation and entrepreneurship : Practice and Principles*. California, CA: HarperCollins Publishers, Inc.

Easterly, W. (2008). Institutions: Top Down or Bottom Up? *American Economic Review, 98*(2), 95-99. URL: https://doi.org/10.1257/aer.98.2.95 (дата звернення: 14.02.2025).

Eberle, W., & Holder, L. (2009, June 8-11, 2009). *Applying Graph-Based Anomaly Detection Approaches to the Discovery of Insider Threats.* Paper presented at

the 2009 IEEE International Conference on Intelligence and Security Informatics, Richardson, TX, USA.

Economic and Financial Crime, Sustainability and Good Governance. (2023). (M. V. Achim Ed.). Cham, Switzerland: Springer. URL: https://doi.org/10.1007/978-3-031-34082-6 (дата звернення: 14.02.2025).

Eischen, K. (2002). *The social impact of informational production : software development as an informational practice*. URL: https://escholarship.org/uc/item/9rp0c3w4 (дата звернення: 14.02.2025).

Elastic: Search More, Spend Less. *Elastic.co*. URL: https://www.elastic.co (дата звернення: 14.02.2025).

Erfani, S. M., Rajasegarar, S., Karunasekera, S., & Leckie, C. (2016). High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning. *Pattern Recognition, 58*, 121-134. URL: https://doi.org/10.1016/j.patcog.2016.03.028 (дата звернення: 14.02.2025).

Ertoz, L., Eilertson, E., Lazarevic, A., Tan, P.-N., Kumar, V., Srivastava, J., & Dokas, P. (2003). Chapter 3. The MINDS - Minnesota Intrusion Detection System. URL: https://www-users.cse.umn.edu/~kumar001/papers/minds_chapter.pdf (дата звернення: 14.02.2025).

Eswar, S., Kannan, R., Vuduc, R., & Park, H. (2021). ORCA: Outlier detection and Robust Clustering for Attributed graphs. *Journal of Global Optimization, 81*(4), 967-989. URL: https://doi.org/10.1007/s10898-021-01024-z (дата звернення: 14.02.2025).

Ewens, W. J., & Brumberg, K. (2023). *Introductory Statistics for Data Analysis*. Cham, Switzerland: Springer. URL: https://doi.org/10.1007/978-3-031-28189-1 (дата звернення: 14.02.2025).

Excel Specifications and Limits. *Microsoft.com*. URL: https://support.microsoft.com/en-us/office/excel-specifications-and-limits-1672b34d-7043-467e-8e27-269d656771c3 (дата звернення: 14.02.2025).

Explainable AI: Foundations, Methodologies and Applications. (2023). (M. Mehta, V. Palade, & I. Chatterjee Eds.). Cham, Switzerland: Springer Nature Switzerland

AG. URL: https://doi.org/10.1007/978-3-031-12807-3 (дата звернення: 14.02.2025).

Financial Crimes: Psychological, Technological, and Ethical Issues. (2016). (M. Dion, D. Weisstub, & J.-L. Richet Eds.): Springer. URL: https://doi.org/10.1007/978-3-319-32419-7 (дата звернення: 14.02.2025).

The flexible AI-powered Search & Discovery platform. *Algolia.com*. URL: https://www.algolia.com (дата звернення: 14.02.2025).

Forensic. *Collinsdictionary.com*. URL: https://www.collinsdictionary.com/dictionary/english/forensic (дата звернення: 14.02.2025).

Fraud and Corruption. Major Types, Prevention, and Control. (2018). (P. C. Kratcoski & M. Edelbacher Eds.). Cham, Switzerland: Springer International Publishing AG. URL: https://doi.org/10.1007/978-3-319-92333-8 (дата звернення: 14.02.2025).

Fraud cases decreased by 21% compared to the previous year. (2025). *Opendatabot.ua*. URL: https://opendatabot.ua/en/analytics/fraud-2024-12 (дата звернення: 14.02.2025).

Fukuyama, F., & Rescanatini, F. (2021). Corruption, elites and power : An overview of international policy efforts to improve the quality of government. In A. Bagenholm, M. Bauhr, M. Grimes, & B. Rothstein (Eds.), *The Oxford Handbook of the Quality of Government* (pp. 472-494). New York, NY: Oxford University Press. URL: https://doi.org/10.1093/oxfordhb/9780198858218.001.0001 (дата звернення: 14.02.2025).

Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). A survey on concept drift adaptation. *ACM Computing Surveys, 46*(4), 1-37. URL: http://dx.doi.org/10.1145/2523813 (дата звернення: 14.02.2025).

Gao, J., Liang, F., Fan, W., Wang, C., Sun, Y., & Han, J. (2010). *On Community Outliers and their Efficient Detection in Information Networks.* Paper presented at the KDD '10: Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining.

Gawthorpe, S. (2018). *Rethinking Corruption in the Czech Republic: A Mixed-Methods Approach to a Systemic Problem.* Charles University, Faculty of Social Sciences, Institute of Sociological Studies, Prague.

Glazunov, V. (2015). Hybrid war in Ukraine: oligarchic discourse. *Skhid, 2*(134), 91-96. URL: https://doi.org/10.21847/1728-9343.2015.2(134).40193 (дата звернення: 14.02.2025).

Goldstein, M., & Uchida, S. (2016). A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data. *PLoS One, 11*(4), e0152173. URL: https://doi.org/10.1371/journal.pone.0152173 (дата звернення: 14.02.2025).

Goldstraw-White, J. (2012). *White-Collar Crime : Accounts of Offending Behaviour*. New York, NY: Palgrave Macmillan. URL: https://doi.org/10.1057/9780230355521 (дата звернення: 14.02.2025).

Gottschalk, P. (2018). *Fraud Investigation: Case Studies of Crime Signal Detection*. New York: Routledge.

Gunnemann, S., Boden, B., Farber, I., & Seidl, T. (2013). Efficient Mining of Combined Subspace and Subgraph Clusters in Graphs with Feature Vectors. In J. Pei, V. S. Tseng, L. Cao, H. Motoda, & G. Xu (Eds.), *Advances in Knowledge Discovery and Data Mining. PAKDD 2013. Lecture Notes in Computer Science* (Vol. 7818). Berlin, Heidelberg: Springer. URL: https://doi.org/10.1007/978-3-642-37453-1_22 (дата звернення: 14.02.2025).

Gupta, I., & Nagpal, G. (2020). *Artificial Intelligence and Expert Systems*. Dulles, VA: David Pallai.

Gupta, P., & Bagchi, A. (2024). *Essentials of Python for Artificial Intelligence and Machine Learning*. Cham, Switzerland: Springer. URL: https://doi.org/10.1007/978-3-031-43725-0 (дата звернення: 14.02.2025).

Han, S., Hu, X., Huang, H., Jiang, M., & Zhao, Y. (2022). ADBench: Anomaly Detection Benchmark. *NeurIPS 2022*, 45. URL: https://doi.org/10.48550/arXiv.2206.09426 (дата звернення: 14.02.2025).

Hasan, H., & Hyland, P. (2001). Using OLAP and multidimensional data for decision making. *IT Professional, 3*(5), 44-50. URL: https://doi.org/10.1109/6294.952980 (дата звернення: 14.02.2025).

Hassan, P., Passing, F., & Goméz, J. M. (2023). ESG Fingerprint: How Big Data and Artificial Intelligence Can Support Investors, Companies, and Stakeholders? In R. Schmidpeter & R. Altenburger (Eds.), *Responsible Artificial Intelligence: Challenges for Sustainable Management* (pp. 219-234). Cham, Switzerland: Springer Nature Switzerland AG. URL: https://doi.org/10.1007/978-3-031-09245-9_11 (дата звернення: 14.02.2025).

Heidenheimer, A., Johnston, M., & Levine, V. (1989). *Political Corruption: A Handbook*. New Brunswick: Transaction Publishers.

Heidenheimer, A. J., & Johnston, M. (2011). *Political Corruption: Concepts and Contexts*. New Brunswick: Transaction Publishers.

Hicken, A., & Mebane, W. R. J. (2017). *A Guide to Elections Forensics: Research and Innovation Grants Working Papers Series*. URL: https://pdf.usaid.gov/pdf_docs/PA00MXR7.pdf (дата звернення: 14.02.2025).

Hlatshwayo, S., Oeking, A., Ghazanchyan, M., Corvino, D., Shukla, A., & Leigh, L. (2018). *The Measurement and Macro-Relevance of Corruption: A Big Data Approach*. IMF.

Hojjati, H., Ho, T. K. K., & Armanfard, N. (2022). Self-Supervised Anomaly Detection: A Survey and Outlook. *Neural Networks, 172*, 1-18. URL: https://doi.org/10.48550/arXiv.2205.05173 (дата звернення: 14.02.2025).

House MD. (2004-2012). *IMDB.com*. URL: https://www.imdb.com/title/tt0412142/

Huggingface : The AI community building the future. *Huggingface.co*. URL: https://huggingface.co/ (дата звернення: 14.02.2025).

Huntington, S. P. (1968). *Modernization and Corruption. Political Order in Changing Societies*. New Haven, Conn: Yale University Press.

Hussain, S. R., Sallam, A. M., & Bertino, E. (2015). *DetAnom*. Paper presented at the Proceedings of the 5th ACM Conference on Data and Application Security and

Privacy. URL: https://doi.org/10.1145/2699026.2699111 (дата звернення: 14.02.2025).

IBM Watson Discovery. *Ibm.com*. URL: https://www.ibm.com/cloud/watson-discovery (дата звернення: 14.02.2025).

Ignatow, G. (2020). *Sociological theory in the digital age*. New York, NY: Routledge.

INDRI: Language modeling meets inference networks. *Lemurproject.org/indri/*. URL: https://www.lemurproject.org/indri/ (дата звернення: 14.02.2025).

Inflection AI : Own your edge. *Inflection.ai*. URL: https://inflection.ai/ (дата звернення: 14.02.2025).

International Handbook on the Economics of Corruption. (2006). (S. Rose-Ackerman Ed.). Cheltenham; Northampton, MA: Edward Elgar Publishing.

International Standard on Auditing 240: The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements. (2010). URL: www.ibr-ire.be/docs/default-source/nl/Documents/regelgeving-en-publicaties/rechtsleer/normen-en-aanbevelingen/ISA-s/nieuwe-en-herziene-ISA-s/New-and-Revised-ISAs-2017/ISA-240.pdf (дата звернення: 14.02.2025).

Introduction to Search with SPHINX. *Sphinxsearch.com*. URL: http://sphinxsearch.com (дата звернення: 14.02.2025).

Ishikawa, K. (1987). *What is total quality control? : The Japanese way*. Englewood Cliffs, NJ: Prentice-Hall. URL: https://archive.org/details/whatistotalquali00ishi/ (дата звернення: 14.02.2025).

Isson, J. P. (2018). *Unstructured Data Analytics: How to Improve Customer Acquisition, Customer Retention, and Fraud Detection and Prevention*. Hoboken, NJ: Wiley.

Jaffri, A., Popa, A., Krensky, P., Hare, J., Bhati, R., Hassanlou, M., & Zhang, T. (2024). Magic Quadrant for Data Science and Machine Learning Platforms. *Gartner.com*. URL: https://www.gartner.com/doc/reprints?id=1-2HVQCAF2&ct=240619&st=sb&trk=dfb33dbf-2fd1-4f79-9b81-44bbcb10c3f3&sc_channel=el (дата звернення: 14.02.2025).

Jessop, B. (2022). State theory. In C. Ansell & J. Torfing (Eds.), *Handbook on Theories of Governance* (pp. 77-88). Cheltenham, UK; Northampton, MA: Edward Elgar Publishing Limited. URL: https://doi.org/10.4337/9781800371972 (дата звернення: 14.02.2025).

Kaiser, K., Rahemtulla, H., & Van den Brink, R. (2016). No Movie, No Map, No Money: Local Road Financing Innovations in the Philippines. *Worldbank.org*. URL: https://blogs.worldbank.org/en/governance/no-movie-no-map-no-money-local-road-financing-innovations-philippines (дата звернення: 14.02.2025).

Kale, V. (2016). *Enhancing Enterprise Intelligence: Leveraging ERP, CRM, SCM, PLM, BPM, and BI*. New York, NY: Auerbach Publications. URL: https://doi.org/10.1201/b19509 (дата звернення: 14.02.2025).

Kangra, K., & Singh, J. (2023). Explainable Artificial Intelligence: Concepts and Current Progression. In A. E. Hassanien, D. Gupta, A. K. Singh, & A. Garg (Eds.), *Explainable Edge AI: A Futuristic Computing Perspective* (pp. 1-17). Cham, Switzerland: Springer Nature Switzerland AG. URL: https://doi.org/10.1007/978-3-031-18292-1_1 (дата звернення: 14.02.2025).

Kaplan, J. (2023). *Crime by the Numbers : A Criminologist's Guide to R*. Boca Raton, FL: CRC Press. URL: https://doi.org/10.1201/9781003279211 (дата звернення: 14.02.2025).

Kejriwal, M. (2023). *Artificial Intelligence for Industries of the Future: Beyond Facebook, Amazon, Microsoft and Google*. Cham, Switzerland: Springer Nature Switzerland AG. URL: https://doi.org/10.1007/978-3-031-19039-1 (дата звернення: 14.02.2025).

Khan, M. H., Andreoni, A., & Roy, P. (2016). Anti-Corruption in Adverse Contexts: A Strategic Approach. *SOAS Working Paper*. URL: http://eprints.soas.ac.uk/23495/1/Anti-Corruption%20in%20Adverse%20Contexts%20(1).pdf (дата звернення: 14.02.2025).

Khan, M. I., & Foley, S. N. (2016). *Detecting anomalous behavior in DBMS logs.* Paper presented at the Proceedings of the 11th International conference on Risks

and Security of Internet and Systems (Roscoff, France, 5th–7th September 2016). CRiSIS2016, Roscoff, France.

Khan, M. I., Foley, S. N., & O'Sullivan, B. (2017). *On database intrusion detection*. Paper presented at the Proceedings of the 2017 the 7th International Conference on Communication and Network Security. URL: https://doi.org/10.1145/3163058.3163068 (дата звернення: 14.02.2025).

Kirby, N., & Wolff, J. (2021). “Quality of Government” : A Philosophical Assessment. In A. Bagenholm, M. Bauhr, M. Grimes, & B. Rothstein (Eds.), *The Oxford Handbook of the Quality of Government* (pp. 42-62). New York, NY: Oxford University Press. URL: https://doi.org/10.1093/oxfordhb/9780198858218.001.0001 (дата звернення: 14.02.2025).

Klimek, P., Jimenez, R., Hidalgo, M., Hinteregger, A., & Thurner, S. (2018). Forensic analysis of Turkish elections in 2017-2018. *PLoS One, 13*(10), e0204975. URL: https://doi.org/ 10.1371/journal.pone.0204975 (дата звернення: 14.02.2025).

Klimek, P., Yegorov, Y., Hanel, R., & Thurner, S. (2012). Statistical detection of systematic election irregularities. *PNAS, 109*(41), 16469-16473. URL: https://doi.org/10.1073/pnas.1210722109 (дата звернення: 14.02.2025).

Kobak, D., Shpilkin, S., & Pshenichnikov, M. S. (2016). Statistical Fingerprints of Electoral Fraud? *Significance, 13*(4), 20-23. URL: https://doi.org/10.1111/j.1740-9713.2016.00936.x (дата звернення: 14.02.2025).

Kobak, D., Shpilkin, S., & Pshenichnikov, M. S. (2020). Suspect Peaks in Russia's “Referendum” Results. *Significance, 17*(5), 8-9. URL: https://doi.org/10.1111/1740-9713.01438 (дата звернення: 14.02.2025).

Köbis, N., Starke, C., & Rahwan, I. (2021). Artificial Intelligence as an Anti-Corruption Tool (AI-ACT) Potentials and Pitfalls for Top-down and Bottom-up Approaches. *Arxiv.org*. URL: https://doi.org/10.48550/arXiv.2102.11567 (дата звернення: 14.02.2025).

Köbis, N., Starke, C., & Rahwan, I. (2022). The promise and perils of using artificial intelligence to fight corruption. *Nature Machine Intelligence, 4*(5), 418-424.

URL: https://doi.org/10.1038/s42256-022-00489-1 (дата звернення: 14.02.2025).

Korstanje, J. (2022). *Machine Learning on Geographical Data Using Python : Introduction into Geodata with Applications and Use Cases*. New York, NY: Apress. URL: https://doi.org/10.1007/978-1-4842-8287-8 (дата звернення: 14.02.2025).

Kryvoshein, V. (2023). Transformation of Political Perceptions in the Age of Information Technologies: Analyzing the Impact on Political Beliefs. *Futurity of Social Sciences*, 20-32. URL: https://doi.org/10.57125/fs.2023.09.20.02 (дата звернення: 14.02.2025).

Kudinov, I., & Yatsyna, Y. (2025). Tools for automating cognitive activities of specialists in the field of monitoring and evaluation of international technical assistance projects. *Center for Independent Social Research*. URL: https://cisr.zp.ua/mel-tools (дата звернення: 25.05.2025).

Kumari, R., Sheetanshu, Singh, M. K., Jha, R., & Singh, N. K. (2016). *Anomaly Detection in Network Traffic using K-mean clustering*. Paper presented at the 3rd International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India. URL: https://doi.org/10.1109/RAIT.2016.7507933 (дата звернення: 14.02.2025).

Lacasa, L., & Fernandez-Gracia, J. (2019). Election Forensics: Quantitative Methods for Electoral Fraud Detection. *Forensic Sci Int, 294*, e19-e22. URL: https://doi.org/ 10.1016/j.forsciint.2018.11.010 (дата звернення: 14.02.2025).

Lai, K.-H., Zha, D., Wang, G., Xu, J., Zhao, Y., Kumar, D., . . . Hu, X. (2021). TODS: An Automated Time Series Outlier Detection System. URL: https://doi.org/10.48550/arXiv.2009.09822 (дата звернення: 14.02.2025).

Lantz, B. (2023). *Machine Learning with R*. Birmingham: Packt Publishing.

Lawless, C. (2022). *Forensic Science: A Sociological Introduction*. Oxon: Routledge. URL: https://doi.org/10.4324/9781003126379 (дата звернення: 14.02.2025).

Lepskyi, M., Kudinov, I., Lepska, N., & Rusetsky, A. (2023). The impact of metacognitive changes of digitalized consciousness on public administration

policy. *Cuestiones Políticas, 41*(79), 253-277. URL: https://doi.org/10.46398/cuestpol.4179.17 (дата звернення: 14.02.2025).

Levin, I., Pomares, J., & Alvarez, R. M. (2016). Using Machine Learning Algorithms to Detect Election Fraud. In *Computational Social Science* (pp. 266-294). URL: https://doi.org/10.1017/cbo9781316257340.012 (дата звернення: 14.02.2025).

Li, D., & Xu, Q. (2022). Research on the Impact of Government Audit on Improving the Innovation Performance of State-Owned Enterprises Under the Background of Big Data. *Frontiers in Business, Economics and Management, 4*(3), 94-100. URL: https://doi.org/10.54097/fbem.v4i3.1274 (дата звернення: 14.02.2025).

Li, X., Liu, S., Li, Z., Han, X., Shi, C., Hooi, B., . . . Cheng, X. (2020). *FlowScope: Spotting Money Laundering Based on Graphs*. Paper presented at the AAAI Conference on Artificial Intelligence, 34(4), 4731-4738. URL: https://doi.org/10.1609/aaai.v34i04.5906 (дата звернення: 14.02.2025).

Lie to Me. (2011-2013). *IMDB.com*. URL: https://www.imdb.com/title/tt1235099

Lima, M. S. M., & Delen, D. (2020). Predicting and Explaining Corruption Across Countries: A Machine Learning Approach. *Government Information Quarterly, 37*(1). URL: https://doi.org/10.1016/j.giq.2019.101407 (дата звернення: 14.02.2025).

Linder, S. H., & Peters, B. G. (1990). An institutional approach to the thory of policy-making: the role of guidance mechanisms in policy formulation. *Journal of Theoretical Politics, 2*(1), 59-83. URL: https://doi.org/10.1177/0951692890002001003 (дата звернення: 14.02.2025).

Liu, C., Gao, Y., Sun, L., Feng, J., Yang, H., & Ao, X. (2022). *User Behavior Pre-training for Online Fraud Detection*. Paper presented at the Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. URL: https://doi.org/10.1145/3534678.3539126 (дата звернення: 14.02.2025).

Liu, G., & Wong, L. (2008). *Effective Pruning Techniques for Mining Quasi-Cliques.* Paper presented at the ECML PKDD 2008, Part II, LNAI 5212, September 15-19, 2008, Antwerp, Belgium.

Liu, J., Bier, E., Wilson, A., Guerra-Gomez, J. A., Honda, T., Sricharan, K., . . . Davies, D. (2015). Graph Analysis for Detecting Fraud, Waste, and Abuse in Health-Care Data. *AI Magazine, 37*(2), 33-46. URL: http://dx.doi.org/10.1609/aimag.v37i2.2630 (дата звернення: 14.02.2025).

Liu, K., Dou, Y., Zhao, Y., Ding, X., Hu, X., Zhang, R., . . . Yu, P. S. (2022). PyGOD: A Python Library for Graph Outlier Detection. URL: https://doi.org/10.48550/arXiv.2204.12095 (дата звернення: 14.02.2025).

López-Iturriaga, F. J., & Sanz, I. P. (2017). Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces. *Social Indicators Research, 140*(3), 975-998. URL: https://doi.org/10.1007/s11205-017-1802-2 (дата звернення: 14.02.2025).

Lu, M., Han, Z., Rao, S. X., Zhang, Z., Zhao, Y., Shan, Y., . . . Jiang, J. (2022). *BRIGHT - Graph Neural Networks in Real-time Fraud Detection.* Paper presented at the Proceedings of the 31st ACM International Conference on Information & Knowledge Management.

Lufkin, B. (2017, 19.10.2017). Could Estonia be the first ‘digital’ country? *BBC News.* URL: https://www.bbc.com/future/article/20171019-could-estonia-be-the-first-digital-country (дата звернення: 14.02.2025).

LUNR: Search made simple. *Lunrjs.com*. URL: https://lunrjs.com (дата звернення: 14.02.2025).

Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q. Z., . . . Akoglu, L. (2022). A *Comprehensive Survey on Graph Anomaly Detection with Deep Learning*. Paper presented at the IEEE Transactions on Knowledge and Data Engineering, 32. URL: https://doi.org/10.1109/TKDE.2021.3118815 (дата звернення: 14.02.2025).

Machine Learning Applications for Accounting Disclosure and Fraud Detection. (2021). (S. Papadakis, A. Garefalakis, C. Lemonakis, C. Chimonaki, & C. Zopounidis Eds.). Hershey, PA: IGI Global.

Mamun, A. A., Azad, A. K., & Pramanik, I. (2023). Crime-Finder: A System for Extraction and Visualization of Crime Data from Bengali Online Newspaper

Articles. In N. Siddique, M. Shamsul, J. Wall, & S. M. Kaiser (Eds.), *Applied Informatics for Industry 4.0* (pp. 97-108). Boca Raton, FL: CRC Press. URL: https://doi.org/10.1201/9781003256069 (дата звернення: 14.02.2025).

Mansour, E., Taha, R., & Taha, N. (2023). The Impact of Internet of Things on the Quality of Financial Reporting. In A. M. A. M. Al-Sartawi, A. Razzaque, & M. M. Kamal (Eds.), *From the Internet of Things to the Internet of Ideas: The Role of Artificial Intelligence: Proceedings of EAMMIS 2022* (pp. 367-374). Cham, Switzerland: Springer Nature Switzerland AG. URL: https://doi.org/10.1007/978-3-031-17746-0_30 (дата звернення: 14.02.2025).

Martin, J. (1977). *Computer data-base organization*. Englewood Cliffs, NJ: IBM Systems Research Institute; Prentice-Hall, Inc.

Massaro, P. (2017). *The internal enemy. A Helsinki Commission staff report on corruption in Ukraine*. URL: https://www.csce.gov/sites/helsinkicommission.house.gov/files/The%20Internal%20Enemy_Final.pdf (дата звернення: 14.02.2025).

Mathew, S., Petropoulos, M., Ngo, H. Q., & Upadhyaya, S. (2010). *A Data-Centric Approach to Insider Attack Detection in Database Systems.* Paper presented at the Recent Advances in Intrusion Detection. RAID 2010. Lecture Notes in Computer Science, Berlin, Heidelberg.

Mebane, W. R. J. (2009). *Note on the Presidential Election in Iran, June 2009*. URL: http://websites.umich.edu/~wmebane/note29jun2009.pdf (дата звернення: 14.02.2025).

Mebane, W. R. J. (2015). *Election Forensics Toolkit DRG Center Working Paper*. URL: https://electionforensics.cps.isr.umich.edu/pdf/report.pdf (дата звернення: 14.02.2025).

Mebane, W. R. J., & Kalinin, K. (2023). Guide to Election Forensics Toolkit. URL: https://electionforensics.cps.isr.umich.edu/election (дата звернення: 14.02.2025).

Mebane, W. R. J., & Klaver, J. (2015). *Election Forensics: Strategies versus Election Frauds in Germany*. URL: http://www.umich.edu/~wmebane/epsa15.pdf (дата звернення: 14.02.2025).

Mebane, W. R. J., & Wall, J. (2015). Election Frauds, Postelection Legal Challenges and Geography in Mexico [Press release]. Retrieved from http://www.umich.edu/~wmebane/apsa15.pdf (дата звернення: 14.02.2025).

Megatrends 2020 and beyond. (2020). URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/megatrends/ey-megatrends-2020-report.pdf (дата звернення: 14.02.2025).

The Mentalist. (2008-2015). *IMDB.com*. URL: https://www.imdb.com/title/tt1196946/ (дата звернення: 14.02.2025).

Mimmack, G. M., Mason, S. J., & Galpin, J. S. (2001). Choice of Distance Matrices in Cluster Analysis: Defining Regions. *Journal of Climate, 14*(12), 2790-2797. URL: https://doi.org/10.1175/1520-0442(2001)014<2790:CODMIC>2.0.CO;2 (дата звернення: 14.02.2025).

Moser, F., Colak, R., Rafiey, A., & Ester, M. (2009). *Mining Cohesive Patterns from Graphs with Feature Vectors.* Paper presented at the Proceedings of the 2009 SIAM International Conference on Data Mining (SDM). URL: https://doi.org/10.1137/1.9781611972795.51 (дата звернення: 14.02.2025).

Muller, E., Sanchez, P. I., Mulle, Y., & Bohm, K. (2013). *Ranking Outlier Nodes in Subspaces of Attributed Graphs.* Paper presented at the 2013 IEEE 29th International Conference on Data Engineering Workshops (ICDEW), Brisbane, QLD, Australia. URL: https://doi.org/10.1109/ICDEW.2013.6547453 (дата звернення: 14.02.2025).

MySQL: Full-Text Search Functions. *Mysql.com*. URL: https://dev.mysql.com/doc/refman/8.0/en/fulltext-search.html (дата звернення: 14.02.2025).

Next-generation AML: 6 Tips to Modernize Your Fight Against Money Laundering. (2023). URL: https://www.sas.com/en/whitepapers/next-generation-aml-110644.html (дата звернення: 14.02.2025).

NLP-Center: NoSketch Engine. *Nlp.fi.muni.cz*. URL: https://nlp.fi.muni.cz/trac/noske (дата звернення: 14.02.2025).

Noerlina, Dewanti, R., Mursitama, T. N., Fairianti, S. P., Kristin, D. M., Sasmoko, . . . Makalew, B. A. (2018). *Development of a Web Based Corruption Case Mapping using Machine Learning with Artificial Neural Network.* Paper presented at the 2018 International Conference on Information Management and Technology (ICIMTech). (дата звернення: 14.02.2025). URL: https://doi.org/10.1109/ICIMTECH.2018.8528150 (дата звернення: 14.02.2025).

Nord, J. H., & Nord, G. D. (1995). Executive information systems : a study and comparative analysis. *Information & Management, 29*(2), 95-106. URL: https://doi.org/10.1016/0378-7206(95)00013-M (дата звернення: 14.02.2025).

Norris, P. (2020). *Rusty Guillotines: Electoral Accountability and Government Corruption*. URL: https://www.pippanorris.com/new-research-papers (дата звернення: 14.02.2025).

Occupational Fraud 2022: A Report to the Nations. (2022). URL: https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf (дата звернення: 14.02.2025).

Odilla, F. (2023). Bots Against Corruption: Exploring the Benefits and Limitations of AI-based Anti-corruption Technology. *Crime, Law and Social Change, 80*, 353-396. URL: https://doi.org/10.1007/s10611-023-10091-0 (дата звернення: 14.02.2025).

Oksha, N. (2019). Empowering Citizens as Watchdogs in Ukraine - Open Government Partnership. URL: https://www.opengovpartnership.org/stories/lessons-from-reformers-empowering-citizens-as-watchdogs-in-ukraine/ (дата звернення: 14.02.2025).

Olken, B. A. (2007). Monitoring Corruption: Evidence from a Field Experiment in Indonesia. *Journal of Political Economy, 115*(2), 200-249. URL: https://doi.org/10.1086/517935 (дата звернення: 14.02.2025).

Open-source Database for Search Applications. *Manticoresearch.com*. URL: https://manticoresearch.com (дата звернення: 14.02.2025).

OpenAI platform. *OpenAI.com*. URL: https://platform.openai.com/overview (дата звернення: 14.02.2025).

Opendatabot. *Opendatabot.ua*. URL: https://opendatabot.ua/ (дата звернення: 14.02.2025).

Pang, G., Shen, C., Cao, L., & Hengel, A. V. D. (2021). Deep Learning for Anomaly Detection: A Review. *ACM Computing Surveys, 54*(2), 1-38. URL: https://doi.org/10.1145/3439950 (дата звернення: 14.02.2025).

Perozzi, B., Akoglu, L., Iglesias Sánchez, P., & Müller, E. (2014). *Focused clustering and outlier detection in large attributed graphs*. Paper presented at the Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining. URL: https://doi.org/10.1145/2623330.2623682 (дата звернення: 14.02.2025).

Petruf, M., Madarász, L., & Kolesár, J. (2011). *Computer Aided Acquisition and Logistic Support.* Paper presented at the 3rd IEEE International Symposium on Logistics and Industrial Informatics Budapest, Hungary. URL: https://doi.org/10.1109/LINDI.2011.6031156 (дата звернення: 14.02.2025).

Pietrzyk-Reeves, D. (2017). Normative political theory. *Teoria Polityki, 1*, 173-185. URL: https://doi.org/10.4467/00000000TP.17.009.6588 (дата звернення: 14.02.2025).

Pinheiro, C. A. R., & McNeill, F. (2014). *Heuristics in Analytics : a Practical Perspective of What Influences Our Analytical World*. Hoboken, New Jersey: Wiley.

Pintar, J., & Hopping, D. (2023). *Information science : the basics*. New York, NY: Routledge. URL: https://doi.org/10.4324/9781003155119 (дата звернення: 14.02.2025).

Power Your Website with the World's Best Search. *Yext.com*. URL: https://www.yext.com (дата звернення: 14.02.2025).

A Powerful Search Experience for Your Website - Without the Learning Curve. *Swiftype.com*. URL: https://swiftype.com (дата звернення: 14.02.2025).

Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2010). Insiders behaving badly : addressing bad actors and their actions. *IEEE Transactions on Information Forensics and Security, 5*(1), 169-179. URL: https://doi.org/10.1109/MSP.2008.87 (дата звернення: 14.02.2025).

Prozorro. *Prozorro.gov.ua*. URL: https://prozorro.gov.ua/ (дата звернення: 14.02.2025).

PyGOD. (2023). *Github.com*. URL: https://github.com/pygod-team/pygod (дата звернення: 14.02.2025).

Python Outlier Detection (PyOD). (2023). *Github.com*. URL: https://github.com/yzhao062/pyod (дата звернення: 14.02.2025).

Rahwan, I., Cebrian, M., Obradovich, N., Bongard, J., Bonnefon, J. F., Breazeal, C., ... Wellman, M. (2019). Machine behaviour. *Nature,* 568(7753), 477-486. URL: https://doi.org/10.1038/s41586-019-1138-y (дата звернення: 14.02.2025).

Ralha, C. G., & Silva, C. V. S. (2012). A Multi-Agent Data Mining System for Cartel Detection in Brazilian Government Procurement. *Expert Systems with Applications, 39*(14), 11642-11656. URL: https://doi.org/10.1016/j.eswa.2012.04.037 (дата звернення: 14.02.2025).

Ringsholm, J. F. (2022a). How I Tested the Hungarian Election for Fraud Using Benford's Law. URL: https://towardsdatascience.com/how-i-tested-the-hungarian-election-for-fraud-using-benfords-law-2d32ea92fe7c (дата звернення: 14.02.2025).

Ringsholm, J. F. (2022b). Hungarian Election Fraud. URL: https://github.com/JensFugl/Hungarian-election-fraud (дата звернення: 14.02.2025).

Rose-Ackerman, S., & Palifka, B. J. (2016). *Corruption and Government: Causes, Consequences, and Reform*. Cambridge: Cambridge University Press. URL: https://doi.org/10.1017/CBO9781139962933 (дата звернення: 14.02.2025).

Rothstein, B. (2021). Quality of Government : Theory and Conceptualization. In A. Bagenholm, M. Bauhr, M. Grimes, & B. Rothstein (Eds.), *The Oxford Handbook of the Quality of Government* (pp. 1-24). New York, NY: Oxford University

Press. URL: https://doi.org/10.1093/oxfordhb/9780198858218.001.0001 (дата звернення: 14.02.2025).

Rozenas, A. (2016). *Package 'spikes'. Detecting Election Fraud from Irregularities in Vote-Share Distributions*. URL: https://cran.r-project.org/web/packages/spikes/spikes.pdf (дата звернення: 14.02.2025).

Rozenas, A. (2017). Detecting Election Fraud from Irregularities in Vote-Share Distributions. *Political Analysis, 25*(1), 41-56. URL: https://doi.org/10.1017/pan.2016.9 (дата звернення: 14.02.2025).

Rudnieva, A. (2024). Innovative Analytical and Statistical Technologies in the Development of Democracy in the State. *Філософія та політологія в контексті сучасної культури, 16*(2), 135-146. URL: https://doi.org/10.15421/352454 (дата звернення: 14.02.2025).

Salehi, M., Mirzaei, H., Hendrycks, D., Li, Y., Rohban, M. H., & Sabokrou, M. (2022). A Unified Survey on Anomaly, Novelty, Open-Set, and Outof-Distribution Detection: Solutions and Future Challenges. 81. URL: https://doi.org/10.48550/arXiv.2110.14051 (дата звернення: 14.02.2025).

Salem, M. B., Hershkop, S., & Stolfo, S. J. (2009). A survey of insider attack detection research. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, & S. Sinclair (Eds.), *Insider Attack and Cyber Security* (pp. 69-90). New York, NY: Springer. URL: https://doi.org/10.1007/978-0-387-77322-3 (дата звернення: 14.02.2025).

Sallam, A., Fadolalkarim, D., Bertino, E., & Xiao, Q. (2016). Data and syntax centric anomaly detection for relational databases. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 6*(6), 231-239. URL: https://doi.org/10.1002/widm.1195 (дата звернення: 14.02.2025).

Schöberlein, J. (2019). *Lessons learned from anticorruption efforts at municipal and city level*. Bergen: U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute. URL: https://www.u4.no/publications/lessons-learned-from-anti-corruption-efforts-at-municipal-and-city-level.pdf (дата звернення: 14.02.2025).

SearchUnify for Sales & Customer Service. *Searchunify.com*. URL: https://www.searchunify.com (дата звернення: 14.02.2025).

Sehwag, V., Chiang, M., & Mittal, P. (2021). SSD: A Unified Framework for Self-Supervised Outlier Detection. *ICLR 2021*. URL: https://doi.org/10.48550/arXiv.2103.12051 (дата звернення: 14.02.2025).

Shakespeare, W. (2017). *The tradegy of Hamlet Prince of Denmark / edited by Barbara W. Mowat, Paul Werstine*. URL: https://socrates.acadiau.ca/courses/engl/rcunningham/resources/Shpe/Hamlet.pdf (дата звернення: 14.02.2025).

Shao, C., Du, X., Yu, J., & Chen, J. (2022). Cluster-Based Improved Isolation Forest. *Entropy (Basel), 24*(5), 17. URL: https://doi.org/10.3390/e24050611 (дата звернення: 14.02.2025).

Sičáková-Beblavá, E., & Beblavý, M. (2007). Prístupy k definovaniu korupcie. *Sociológia, 39*(4), 316-336.

Siegel, A. F. (2016). *Practical Business Statistics*. London: Academic Press.

Silver, N. (2009, 15.06.2009). Iranian Election Results by Province [UPDATED]. *Five Thirty Eight Politics.* URL: http://fivethirtyeight.com/features/iranian-election-results-by-province/ (дата звернення: 14.02.2025).

Since the beginning of the large-scale war, 6,800 corruption convictions have been handed down. (2024, 29.10.2024). *Opendatabot.ua*. URL: https://opendatabot.ua/en/analytics/corrupted-officials-2024 (дата звернення: 14.02.2025).

Solr is the popular, blazing-fast, open source enterprise search platform built on Apache Lucene. *Lucene.apache.org*. URL: https://lucene.apache.org/solr/ (дата звернення: 14.02.2025).

Starke, C., Naab, T. K., & Scherer, H. (2016). Free to Expose Corruption: The Impact of Media Freedom, Internet Access, and Governmental Online Service Delivery on Corruption. *International Journal of Communication, 10*, 4702–4722. URL: https://ijoc.org/index.php/ijoc/article/view/5712/1793 (дата звернення: 14.02.2025).

Statistical Anomalies in Russian Elections. (2024). *Github.com*. URL: https://github.com/dkobak/elections (дата звернення: 14.02.2025).

Steif, K. (2022). *Public Policy Analytics: Code and Context for Data Science in Government*. Boca Raton, FL CRC Press. URL: https://doi.org/10.1201/9781003054658 (дата звернення: 14.02.2025).

Suthaharan, S. (2016). *Machine Learning Models and Algorithms for Big Data Classification*. New York: Springer Science+Business Media. URL: https://doi.org/10.1007/978-1-4899-7641-3 (дата звернення: 14.02.2025).

TODS: Automated Time-series Outlier Detection System. (2023). *Github.com*. URL: https://github.com/datamllab/tods (дата звернення: 14.02.2025).

Tureckova, K. (2021). Specific types and categorizations of brownfields : synthesis of individual approaches. *Geographia Technica, 16*(2), 29-39. URL: http://dx.doi.org/10.21163/GT_2021.162.03 (дата звернення: 14.02.2025).

Udovyka, L. H., & Kaluhina, I. O. (2025). The Concept of Corruption: Scientific Approaches and Legal Interpretation. *Juridical scientific and electronic journal,* 1, 67-71. URL: https://doi.org/10.32782/2524-0374/2025-1/13 (дата звернення: 14.02.2025).

Using Machine Learning for Anti-Corruption Risk and Compliance. (2021). Coalition for Integrity. URL: https://www.coalitionforintegrity.org/wp-content/uploads/2021/04/Using-Machine-Learning-for-Anti-Corruption-Risk-and-Compliance.pdf (дата звернення: 14.02.2025).

Varoufakis, Y. (2024). *Technofeudalism: what killed capitalism*. New York, NY: Melville House.

Vaughan, G. (2020). Efficient Big Data Model Selection with Applications to Fraud Detection. *International Journal of Forecasting, 36*(3), 1116-1127. URL: https://doi.org/10.1016/j.ijforecast.2018.03.002 (дата звернення: 14.02.2025).

Vincent, J., Fei, S., Arnaud, S., Bijan, R., Yanlei, D., & Nesime, T. (2021). Exathlon: A Benchmark for Explainable Anomaly Detection over Time Series. *Proceedings of the VLDB Endowment, 14*(11), 2613-2626. URL: https://doi.org/10.14778/3476249.3476307 (дата звернення: 14.02.2025).

Vona, L. W. (2017). *Fraud Data Analytics Methodology : the Fraud Scenario Approach to Uncovering Fraud in Core Business Systems*. Hoboken, New Jersey: Wiley.

Welcome to Apache Lucene. *Lucene.apache.org*. URL: https://lucene.apache.org (дата звернення: 14.02.2025).

Welcome to the Terrier IR Platform. *Terrier.org*. URL: http://terrier.org (дата звернення: 14.02.2025).

Wells, J. T. (2014). *Principles of Fraud Examination*. Hoboken, NJ: Wiley.

Wells, J. T. (2017). *Corporate Fraud Handbook. Prevention and Detection*. Hoboken, New Jersey: Wiley.

Wells, J. T. (2018). *International Fraud Handbook*. Hoboken, New Jersey: Wiley.

What is Corruption? (2023). *Transparency.org*. URL: https://www.transparency.org/en/what-is-corruption (дата звернення: 14.02.2025).

Wiener, N. (1954). *The human use of human beings : cybernetics and society*. Boston, MA: Houghton Mifflin.

Xapian: Open Source Search Engine Library. *Xapian.org*. URL: https://xapian.org (дата звернення: 14.02.2025).

Xu, X., Mao, Z. M., & Halderman, J. A. (2011). *Internet censorship in China : where does the filtering occur?* Paper presented at the Passive and Active Measurement Conference, Atlanta, GA. URL: http://www.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf (дата звернення: 14.02.2025).

Yatsyna, Y., & Kudinov, I. (2023). Innovative Analytical and Statistical Technology in Election Forensics. *Regional Formation and Development Studies, 2*(40), 28-42. URL: https://doi.org/10.15181/rfds.v40i2.2528 (дата звернення: 14.02.2025).

Yatsyna, Y., & Kudinov, I. (2025). Tools for automating forensic activities in risk management, corporate governance, and compliance. *Union of Social Engineers of Ukraine*. URL: https://www.useu.org.ua/forensic-tools (дата звернення: 14.02.2025).

YouControl : Перевіряйте контрагентів та стежте за їх змінами. *Youcontrol.com.ua*. URL: https://youcontrol.com.ua/ (дата звернення: 14.02.2025).

YT-dlp. *Github.com*. URL: https://github.com/yt-dlp/yt-dlp (дата звернення: 14.02.2025).

Zemankova, A. (2019). *Artificial Intelligence in Audit and Accounting: Development, Current Trends, Opportunities and Threats - Literature Review.* Paper presented at the 2019 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO). URL: https://doi.org/10.1109/iccairo47923.2019.00031 (дата звернення: 14.02.2025).

Zhang, M., Alvarez, R. M., & Levin, I. (2019). Election Forensics: Using Machine Learning and Synthetic Data for Possible Election Anomaly Detection. *PLoS One, 14*(10), e0223950. URL: https://doi.org/10.1371/journal.pone.0223950 (дата звернення: 14.02.2025).

Zhao, Y., Chen, G. H., & Jia, Z. (2022). TOD: GPU-accelerated Outlier Detection via Tensor Operations. *Proceedings of the VLDB Endowment, 16*(1). URL: https://doi.org/10.48550/arXiv.2110.14007 (дата звернення: 14.02.2025).

Zhao, Y., Hu, X., Cheng, C., Wang, C., Wan, C., Wang, W., ... Akoglu, L. (2021). SUOD: Accelerating Large-Scale Unsupervised Heterogeneous Outlier Detection. *Proceedings ofthe 4th MLSys Conference*. URL: https://doi.org/10.48550/arXiv.2003.05731 (дата звернення: 14.02.2025).

Zhao, Y., Nasrullah, Z., & Li, Z. (2019). PyOD: A Python Toolbox for Scalable Outlier Detection. *Journal of Machine Learning Research, 20*, 1-7. URL: https://doi.org/10.48550/arXiv.1901.01588 (дата звернення: 14.02.2025).

Zhou, Y., Cheng, H., & Yu, J. X. (2009). *Graph Clustering Based on Structural/Attribute Similarities.* Paper presented at the Proceedings of the VLDB Endowment. URL: https://doi.org/10.14778/1687627.1687709 (дата звернення: 14.02.2025).

ДОДАТКИ

Додаток А

А.1 – Python-скрипт автоматизованого пошуку публікацій в форматі .pdf в пошуковій системі Google

search_pdf.py

```
# 📚 Script for PDF search in Google

import requests
import pandas as pd
import os
import json
import time
from datetime import datetime
from concurrent.futures import ThreadPoolExecutor

# Paths to files containing the API key and search engine ID
base_dir = os.path.dirname(os.path.abspath(__file__))  # Defines folder of the script
api_key_file = os.path.join(base_dir, 'keys', 'api.txt')
engine_id_file = os.path.join(base_dir, 'keys', 'engine.txt')

# Check if the API key file exists
if not os.path.exists(api_key_file):
    print(f"❌ File {api_key_file} not found.")
    exit(1)

# Check if the search engine ID file exists
if not os.path.exists(engine_id_file):
    print(f"❌ File {engine_id_file} not found.")
    exit(1)

# Read the API key from the file
with open(api_key_file, 'r') as file:
    api_key = file.read().strip()

# Read the search engine ID from the file
with open(engine_id_file, 'r') as file:
    cx = file.read().strip()

# Read keywords from the "keywords.txt" file
keywords_file = 'keywords.txt'

# Check if the keywords file exists
if not os.path.exists(keywords_file):
    print(f"❌ File {keywords_file} not found.")
    exit(1)

with open(keywords_file, 'r') as file:
    keywords = [line.strip() for line in file if line.strip() and not
line.startswith("#")]
```

```
# Ask the user how many results they want per keyword
max_results = int(input("🔢 Enter the number of results per keyword: "))

# Main folder for saving all results
main_folder = '!search_pdf'
os.makedirs(main_folder, exist_ok=True)

# Current date and time for query marking
current_time = datetime.now().strftime('%Y-%m-%d %H-%M')

def fetch_data(keyword):
    """Function to fetch and process data for a given keyword."""
    print(f"🔎 Processing keyword: {keyword}")

    keyword_folder = os.path.join(main_folder, f"{current_time} {keyword}")
    os.makedirs(keyword_folder, exist_ok=True)

    data = []
    start_index = 1

    while len(data) < max_results:
        query = f'{keyword} filetype:pdf'
        url =
f"https://www.googleapis.com/customsearch/v1?q={query}&key={api_key}&cx={cx}&start={star
t_index}"

        response = requests.get(url)
        results = response.json()

        if 'items' in results:
            for i, item in enumerate(results['items']):
                title = item.get('title', 'No title')
                link = item.get('link', 'No link')
                snippet = item.get('snippet', 'No description')
                timestamp = datetime.now().strftime('%Y-%m-%d %H:%M:%S')
                status = 'Not Attempted'

                if link.endswith('.pdf'):
                    try:
                        pdf_response = requests.get(link, timeout=10)
                        pdf_response.raise_for_status()
                        pdf_name = os.path.join(keyword_folder, f"file_{len(data) +
1}.pdf")
                        with open(pdf_name, 'wb') as f:
                            f.write(pdf_response.content)
                        status = '✅ Successfully Downloaded'
                        print(f"✅ File {pdf_name} downloaded successfully.")
                    except requests.exceptions.Timeout:
                        status = '⏳ Download Timeout'
                        print(f"⏳ Timeout when downloading file: {link}")
                    except requests.exceptions.RequestException as e:
                        status = f"❌ Download Error: {e}"
                        print(f"❌ Error downloading file {link}: {e}")

                data.append([len(data) + 1, title, snippet, link, status, timestamp])
                if len(data) >= max_results:
                    break

            start_index += 10
```

```
        else:
            print("⚠️ No more search results.")
            break

    df = pd.DataFrame(data, columns=['Index', 'Title', 'Description', 'Link', 'Status',
'Timestamp'])
    excel_file_path = os.path.join(keyword_folder,
f'pdf_files_data_{current_time}.xlsx')
    df.to_excel(excel_file_path, index=False, engine='openpyxl')
    print(f"✅ Done! Saved {len(data)} files and data for keyword '{keyword}'.")

def main():
    """Main function to execute multi-threaded search."""
    with ThreadPoolExecutor(max_workers=5) as executor:
        executor.map(fetch_data, keywords)
    print("✅ Processing of all keywords is complete.")

if __name__ == "__main__":
    main()
```

А.2 – Python-скрипт автоматизованого пошуку публікацій в форматі .pdf в репозиторії Google Academia (search_scholar.py, search_missing.py)

search_scholar.py

```
# 📚 Script for PDF search in Google Scholar
import os
import requests
from scholarly import scholarly
import pandas as pd
from datetime import datetime

# 📄 File containing keywords
keywords_file = 'keywords.txt'

# 📁 Folder name for saving results and files
output_folder = '!search_scholar'

# 🛠️ Create the main folder if it does not exist
os.makedirs(output_folder, exist_ok=True)

# ⏰ Current date and time for query marking
current_time = datetime.now().strftime('%Y-%m-%d %H-%M')

# 📥 Reading keywords from the file
with open(keywords_file, 'r', encoding='utf-8') as file:
    keywords = [line.strip() for line in file if line.strip()]

# ❓ Ask the user how many results they want per keyword
desired_results = int(input("🔢 Enter the number of results per keyword: "))

# 📦 List to store all retrieved data
all_data = []

# 🔁 Loop through each keyword
for keyword in keywords:
    if keyword.startswith("#"):
        print(f"⏭️ Skipping keyword: {keyword}")
        continue

    print(f"\n🔎 Processing keyword: {keyword}")

    # 📁 Create a subfolder for the current keyword
    keyword_folder = os.path.join(output_folder, f"{current_time} {keyword}")
    os.makedirs(keyword_folder, exist_ok=True)

    # 🔍 Execute the search query in Google Scholar
    search_query = scholarly.search_pubs(keyword)

    # 📄 Collect data for the current keyword
    data = []
    for i, result in enumerate(search_query):
        timestamp = datetime.now().strftime('%Y-%m-%d %H:%M:%S')

        title = result.get('bib', {}).get('title', 'No title')
        authors = result.get('bib', {}).get('author', 'No authors')
```

```
        abstract = result.get('bib', {}).get('abstract', 'No abstract')
        year = result.get('bib', {}).get('pub_year', 'No year')
        journal = result.get('bib', {}).get('venue', 'No journal')
        url = result.get('pub_url', 'No URL')

        status = '📄 Not a PDF or no download attempted'
        if url.endswith('.pdf'):
            try:
                pdf_response = requests.get(url, timeout=10)
                pdf_response.raise_for_status()

                pdf_name = os.path.join(keyword_folder, f"file_{i + 1}.pdf")
                with open(pdf_name, 'wb') as pdf_file:
                    pdf_file.write(pdf_response.content)

                status = '✅ PDF successfully downloaded'
                print(f"📥 File downloaded: {pdf_name}")
            except requests.exceptions.RequestException as e:
                status = f"❌ Download error: {e}"
                print(f"⚠️ Error downloading {url}: {e}")

        data.append([i + 1, title, authors, year, journal, abstract, url, status,
timestamp, keyword])

        if len(data) >= desired_results:
            break

    if len(data) < desired_results:
        print(f"⚠️ Only {len(data)} results found for '{keyword}', expected
{desired_results}.")

    all_data.extend(data)

# 📊 Create DataFrame
df = pd.DataFrame(all_data, columns=['Index', 'Title', 'Authors', 'Year', 'Journal',
'Abstract', 'URL', 'Status', 'Timestamp', 'Keyword'])

# 💾 Save to Excel
excel_file_path = os.path.join(output_folder, f'scholar_results_{current_time}.xlsx')
df.to_excel(excel_file_path, index=False)

print(f"\n🎉 Done! Results and files are saved in: 📁 '{output_folder}'")
```

search_missing.py

```
# Script to download missing pdf-files of search_scholar script
import os
import pandas as pd
import webbrowser

def list_xlsx_files(directory):
    """List all .xlsx files in the specified directory."""
    return [f for f in os.listdir(directory) if f.endswith('.xlsx')]

def process_failed_downloads(file_path):
    """Processes the file and opens links for manual PDF download."""
    df = pd.read_excel(file_path)
```

```
    if 'Status' not in df.columns or 'URL' not in df.columns or 'Index' not in
df.columns or 'Title' not in df.columns:
        print("⚠️ The file does not contain the required columns (Status, URL, Index,
Title). Check its structure.")
        return

    failed_records = df[df['Status'].isin(['Not Attempted', 'Failed'])]

    if failed_records.empty:
        print("✅ All files have been successfully downloaded, nothing to process.")
        return

    for _, row in failed_records.iterrows():
        index = row['Index']
        title = row['Title']
        url = row['URL']

        print(f"🌐 Opening link {url} for article '{title}' (Record #{index})")
        webbrowser.open(url)

        input("⏬ After downloading the file, press Enter to proceed to the next
link...")

    print("🎉 Processing complete!")

def main():
    directory = input("📂 Enter the path to the directory containing .xlsx files:
").strip()
    if not os.path.isdir(directory):
        print("❌ The specified path does not exist. Check it and try again.")
        return

    xlsx_files = list_xlsx_files(directory)

    if not xlsx_files:
        print("⚠️ No .xlsx files found in the specified folder.")
        return

    print("📄 Available .xlsx files:")
    for i, file in enumerate(xlsx_files):
        print(f"{i + 1}. {file}")

    try:
        choice = int(input("🔢 Enter the number of the file you want to process: ")) - 1
    except ValueError:
        print("❌ Invalid input. Please enter a number.")
        return

    if 0 <= choice < len(xlsx_files):
        file_path = os.path.join(directory, xlsx_files[choice])
        process_failed_downloads(file_path)
    else:
        print("❌ Invalid file selection.")

if __name__ == "__main__":
    main()
```

А.3 – Python-скрипт автоматизованого пошуку відео в YouTube

search_youtube.py

```
# 🎥🔎 YouTube Query Tool: Find Videos by Keyword

import os
import pandas as pd
from googleapiclient.discovery import build
from datetime import datetime

# 🔑 Function to read API key from a file
def get_api_key(file_path):
    try:
        with open(file_path, 'r') as file:
            api_key = file.read().strip()
        return api_key
    except FileNotFoundError:
        print(f"🚫 File {file_path} not found.")
        return None

# 📂 Function to read search queries from a file
def get_search_queries(file_path):
    try:
        with open(file_path, 'r', encoding='utf-8') as file:
            queries = [line.strip() for line in file.readlines()]
        return queries
    except FileNotFoundError:
        print(f"🚫 File {file_path} not found.")
        return []

# 📺 Function to get the channel handle from channel ID
def get_channel_handle(youtube, channel_id):
    request = youtube.channels().list(
        part='snippet',
        id=channel_id
    )
    response = request.execute()
    items = response.get('items', [])
    if items:
        custom_url = items[0]['snippet'].get('customUrl')
        if custom_url:
            return f"@{custom_url}"
    return None

# 🔍 Function to perform YouTube search
def youtube_search(query, api_key, max_results):
    youtube = build('youtube', 'v3', developerKey=api_key)

    videos = []
    next_page_token = None
    total_results = 0

    while total_results < max_results:
        request = youtube.search().list(
            q=query,
            part='snippet',
            type='video',
```

```
            maxResults=min(50, max_results - total_results),
            pageToken=next_page_token
        )
        response = request.execute()

        # 📩 Processing search results
        for item in response['items']:
            channel_id = item['snippet']['channelId']
            channel_url = f"https://www.youtube.com/channel/{channel_id}"
            channel_handle = get_channel_handle(youtube, channel_id)
            channel_handle_url = f"https://www.youtube.com/{channel_handle}" if
channel_handle else channel_url

            # 🕒 Get current timestamp
            timestamp = datetime.now().strftime('%Y-%m-%d %H:%M:%S')

            video_data = {
                'title': item['snippet']['title'],
                'description': item['snippet']['description'],
                'channel': item['snippet']['channelTitle'],
                'video_id': item['id']['videoId'],
                'url': f"https://www.youtube.com/watch?v={item['id']['videoId']}",
                'channel_url': channel_url,
                'channel_handle_url': channel_handle_url,
                'timestamp': timestamp
            }
            videos.append(video_data)

        total_results += len(response['items'])
        next_page_token = response.get('nextPageToken')

        if not next_page_token:
            break

    return videos

# 📊 Function to save data into an Excel file
def save_to_excel(videos, query):
    output_folder = "!search_youtube"
    if not os.path.exists(output_folder):
        os.makedirs(output_folder)

    # ⏳ Get current date and time for file naming
    current_time = datetime.now().strftime('%Y-%m-%d %H-%M')

    # 📝 Create filename with timestamp
    file_name = os.path.join(output_folder, f"{query}_{current_time}.xlsx")
    df = pd.DataFrame(videos)
    df.to_excel(file_name, index=False)
    print(f"✅ Results saved in: {file_name}")

# 🚀 Main program execution
if __name__ == '__main__':
    # 🔑 Read API key from file
    api_key_path = "./Code/keys/api_yt_2.txt"
    api_key = get_api_key(api_key_path)

    if api_key:
        # 📂 Read search queries from file
```

```
    queries_file_path = "keywords.txt"
    queries = get_search_queries(queries_file_path)

    if queries:
        # 🔢 Ask the user how many results they want per keyword
        max_results = int(input("🔢 Enter the number of results per keyword: "))

        for query in queries:
            # ⏭️ Skip keywords starting with #
            if query.startswith("#"):
                print(f"⚠️ Skipping keyword: {query}")
                continue

            print(f"🔍 Searching for: {query}")
            videos = youtube_search(query, api_key, max_results)
            save_to_excel(videos, query)
    else:
        print("🚫 Keywords file is empty or not found.")
else:
    print("🚫 Failed to retrieve API key.")
```

А.4 – Python-скрипт автоматизованого пошуку даних на YouTube-каналах

youtube_channels.py

```
# 🎥🔎 YouTube channels data downloader

import os
import subprocess
import pandas as pd
import json

# 📄 Path to the file with YouTube channel names
channels_file = 'youtube.txt'

# 📁 Directory where JSON files will be saved
directory = "./!youtube_downloader/"
os.makedirs(directory, exist_ok=True)

# 📩 Reading channel list from youtube.txt
with open(channels_file, 'r') as file:
    channels = [line.strip() for line in file if line.strip()]

# 🔁 Iterate over each channel
for channel in channels:
    # 📝 Define filename for saving channel data
    json_filename = f"{channel}.json"
    json_filepath = os.path.join(directory, json_filename)

    # ▶️ Command to fetch channel data using yt-dlp
    command = ['yt-dlp', '-j', f"https://www.youtube.com/{channel}"]

    try:
        # ⚙️ Execute command and write output to file
        with open(json_filepath, 'w') as output_file:
            subprocess.run(command, stdout=output_file, check=True)
        print(f"✅ Data from channel '{channel}' saved to: {json_filepath}")
    except subprocess.CalledProcessError as e:
        print(f"❌ Error fetching data from channel '{channel}': {e}")

# 🔄 After downloading, convert JSON files to Excel

# 📂 Loop through all JSON files in the directory
for filename in os.listdir(directory):
    if filename.endswith(".json"):  # 📎 Only process .json files
        filepath = os.path.join(directory, filename)

        # 📖 Read the content of the JSON file
        with open(filepath, 'r') as file:
            content = file.read()

        # 🧩 Try splitting content into multiple JSON objects if needed
        json_objects = content.strip().split('\n')

        data_frames = []
        for json_str in json_objects:
```

```
            try:
                # 🔍 Parse each JSON string into a dictionary
                json_data = json.loads(json_str)
                # 📄 Convert dictionary to DataFrame
                df = pd.DataFrame([json_data])
                data_frames.append(df)
            except json.JSONDecodeError as e:
                print(f"⚠️ Error parsing JSON from file '{filename}': {e}")

        # 📊 Combine all DataFrames into one
        if data_frames:
            combined_df = pd.concat(data_frames, ignore_index=True)
            # 💾 Save as Excel file using the same name as the JSON file
            excel_path = os.path.join(directory,
f"{os.path.splitext(filename)[0]}.xlsx")
            combined_df.to_excel(excel_path, index=False)
            print(f"📈 Saved Excel file: {excel_path}")
        else:
            print(f"🚫 No data to save from file: {filename}")

# ✅ Completion message
print("🎉 Processing complete.")
```

A.5 – Python-скрипт автоматизованого завантаження відео з YouTube

video_downloader.py

```
# ▶️  YouTube Video downloader

import os
import subprocess

# 📄 Path to the file containing video URLs
url_file = './ Code/video.txt'  # List of video URLs and optional titles
output_folder = './Code/!video3'  # 📁 Folder to save downloaded video/audio

# 📎 Check if the URL file exists
if not os.path.exists(url_file):
    print(f"❌ File not found: {url_file}")
    exit()

# 📁 Create output folder if it doesn't exist
os.makedirs(output_folder, exist_ok=True)

# ❓ Ask the user for download type
download_option = input(
    "📥 Choose download option:\n"
    "1️⃣ – Download video (AVI, with optional MOV conversion)\n"
    "2️⃣ – Download only MP3 files\n"
    "➡ Enter 1 or 2: "
).strip()

# 🧪 Validate input
if download_option not in ('1', '2'):
    print("⚠️ Invalid choice. Please try again.")
    exit()

# 🎶 MP3-only mode
if download_option == '2':
    print("🎧 Downloading only MP3 files...")
    with open(url_file, 'r', encoding='utf-8') as file:
        for line in file:
            line = line.strip()
            if line:
                parts = line.split(' ', 1)
                url = parts[0].strip()
                title = parts[1].strip() if len(parts) > 1 else "untitled"

                output_path_mp3 = os.path.join(output_folder, f"{title}.mp3")
                command_mp3 = f"yt-dlp -x --audio-format mp3 -o \"{output_path_mp3}\"
{url}"
                subprocess.run(command_mp3, shell=True)
                print(f"✅ MP3 saved: {output_path_mp3}")
    print("🎉 All MP3 tasks completed!")
    exit()

# 🎥 Ask about MOV conversion
convert_to_mov = input(
    "🔄 Do you want to convert video files to .mov format? (1 = yes, 0 = no): "
).strip()
```

```
if convert_to_mov not in ('1', '0'):
    print("⚠️ Invalid choice. Please try again.")
    exit()

convert_to_mov = convert_to_mov == '1'

# 🔊 Ask about also downloading MP3
download_mp3 = input(
    "➕ Do you want to also download MP3 audio? (1 = yes, 0 = no): "
).strip()

if download_mp3 not in ('1', '0'):
    print("⚠️ Invalid choice. Please try again.")
    exit()

download_mp3 = download_mp3 == '1'

# 📽️ Download video in AVI format
print("📽️ Downloading videos in AVI format...")
with open(url_file, 'r', encoding='utf-8') as file:
    for line in file:
        line = line.strip()
        if line:
            parts = line.split(' ', 1)
            url = parts[0].strip()
            title = parts[1].strip() if len(parts) > 1 else "untitled"

            output_path_avi = os.path.join(output_folder, f"{title}.avi")
            command_avi = f"yt-dlp -f bestvideo[ext=mp4]+bestaudio[ext=m4a]/best --
merge-output-format avi -o \"{output_path_avi}\" {url}"
            subprocess.run(command_avi, shell=True)
            print(f"✅ AVI saved: {output_path_avi}")

            # 🎶 Optional MP3 download
            if download_mp3:
                output_path_mp3 = os.path.join(output_folder, f"{title}.mp3")
                command_mp3 = f"yt-dlp -x --audio-format mp3 -o \"{output_path_mp3}\"
{url}"
                subprocess.run(command_mp3, shell=True)
                print(f"✅ MP3 saved: {output_path_mp3}")

# 🔁 Optional MOV conversion
if convert_to_mov:
    print("🎬 Converting AVI files to MOV format...")
    for file_name in os.listdir(output_folder):
        if file_name.endswith(".avi"):
            input_file = os.path.join(output_folder, file_name)
            output_file = os.path.join(output_folder, os.path.splitext(file_name)[0] +
".mov")

            convert_command = f"ffmpeg -i \"{input_file}\" -c:v libx264 -preset slow -
crf 22 -c:a aac -b:a 128k \"{output_file}\""
            subprocess.run(convert_command, shell=True)
            print(f"🎞️ MOV saved: {output_file}")

print("🎉 All tasks completed successfully!")
```

А.6 – Python-скрипт автоматизованого стенографування із використанням сервісу ШІ AssemblyAI

transcriber.py

```
# 📝 Transcriber

import assemblyai as aai
import os
import subprocess

# 🔑 Path to the API key file
api_key_file = './Code/keys/api_assembly.txt'
# 🎵 Folder containing audio files for transcription
audio_folder = './Code/!video3'
# 📄 Folder for saving transcribed text files
text_folder = './Code/!text'

# 🚨 Check if the API key file exists
if not os.path.exists(api_key_file):
    print(f"❌ Error: API key file '{api_key_file}' not found.")
    exit(1)

# 🔑 Read API key from file
with open(api_key_file, 'r') as file:
    api_key = file.read().strip()

# 🔧 Set API key for AssemblyAI
aai.settings.api_key = api_key
transcriber = aai.Transcriber()

# 📁 Ensure the text output folder exists
if not os.path.exists(text_folder):
    os.makedirs(text_folder)

# 🔄 Loop for processing files
while True:
    # 📂 Find audio files in the folder
    files = [f for f in os.listdir(audio_folder) if f.endswith(('.mp3', '.mp4', '.wav',
'.m4a'))]

    # 🚨 Check if any files are available for transcription
    if not files:
        print(f"⚠️ No audio files found in '{audio_folder}'.")
        exit(1)

    # 📜 Display available files
    print("\n🎤 Available files for transcription:")
    for i, file in enumerate(files):
        print(f"{i + 1}: {file}")

    # 🎯 Select a file for transcription
    try:
        file_index = int(input("🔢 Enter the file number for transcription: ").strip()) -
1
        if file_index < 0 or file_index >= len(files):
```

```
        print("⚠️ Invalid file selection. Try again.")
        continue
except ValueError:
    print("⚠️ Please enter a valid number.")
    continue

# 📌 Selected file
selected_file = os.path.join(audio_folder, files[file_index])

# 🌍 Select transcription language mode
language_choice = input(
    "🗣️ Choose the recording language:\n"
    "1 - English (with speaker identification)\n"
    "2 - Ukrainian or Russian (text segmented by sentences)\n"
    "Enter 1 or 2: "
).strip()

if language_choice == '1':
    # 🎙️ Configuration for English recordings with speaker identification
    config = aai.TranscriptionConfig(speaker_labels=True)

    # 🚀 Perform transcription
    transcript = transcriber.transcribe(selected_file, config=config)

    # 📄 Generate output filename based on the audio file name
    output_filename = os.path.splitext(files[file_index])[0] + ".txt"
    output_filepath = os.path.join(text_folder, output_filename)

    # 📝 Save transcription to a text file
    with open(output_filepath, 'w', encoding='utf-8') as f:
        for utterance in transcript.utterances:
            f.write(f"Speaker {utterance.speaker}: {utterance.text}\n")

    print(f"✅ Transcription saved: {output_filepath}")

elif language_choice == '2':
    # 📝 Configuration for other languages (without speaker identification)
    config = aai.TranscriptionConfig(
        speech_model=aai.SpeechModel.best,
        language_detection=True
    )

    # 🚀 Perform transcription
    transcript = transcriber.transcribe(selected_file, config)

    # 🧯 Check for transcription errors
    if transcript.status == aai.TranscriptStatus.error:
        print(f"❌ Transcription failed for {files[file_index]}: {transcript.error}")
    else:
        # 📄 Generate output filename based on the audio file name
        output_filename = os.path.splitext(files[file_index])[0] + ".txt"
        output_filepath = os.path.join(text_folder, output_filename)

        # 📝 Save transcription to a text file
        with open(output_filepath, 'w', encoding='utf-8') as f:
            for sentence in transcript.get_sentences():
                f.write(sentence.text + "\n")
```

```
            print(f"✅ Transcription saved: {output_filepath}")

    else:
        print("⚠️ Invalid language selection. Try again.")
        continue

    # 🔄 Ask if another file should be transcribed
    another_file = input("\n🔁 Do you want to transcribe another file? Enter 1 for yes, 0
for no: ").strip()
    if another_file != '1':
        print("🏁 Transcription process completed.")
        break
```

А.7 – Python-скрипт автоматизованого перекладу тексту із використанням сервісу ШІ OpenAI

translator.py

```
# Translator

import json
import os
from openai import OpenAI
import re

# 🔑 Path to the API key file
api_key_file = './Code/keys/api_openai.txt'

# 🚨 Check if the API key file exists
if not os.path.exists(api_key_file):
    print(f"❌ Error: API key file '{api_key_file}' not found.")
    exit()

# 🔑 Read API key from file
with open(api_key_file, 'r') as file:
    api_key = file.read().strip()

# 🤖 Initialize OpenAI client
client = OpenAI(api_key=api_key)

# 📝 System prompt selection based on language
def get_system_prompt(language):
    if language == "ua":
        return "You are a language expert, your job is to translate from English to
Ukrainian."
    elif language == "en":
        return "You are a language expert, your job is to translate from Ukrainian to
English."
    elif language == "ru-en":
        return "You are a language expert, your job is to translate from Russian to
English."
    elif language == "ru-ua":
        return "You are a language expert, your job is to translate from Russian to
Ukrainian."

# ✂️ Function to split text into sentence-based chunks
def split_text_by_sentences(text, max_tokens=3000):
    sentences = re.split(r'(?<!\...)(?<=\.|\?)\s', text)  # Split text into sentences
    chunks = []
    current_chunk = ""

    for sentence in sentences:
        if len(current_chunk) + len(sentence) > max_tokens:
            chunks.append(current_chunk.strip())
            current_chunk = sentence
        else:
            current_chunk += " " + sentence

    if current_chunk:
        chunks.append(current_chunk.strip())
```

```
    return chunks

# 🔄 Function to translate text using GPT-4
def translate_text(text, system_prompt):
    try:
        chat_completion = client.chat.completions.create(
            messages=[
                {"role": "system", "content": system_prompt},
                {"role": "user", "content": f"Translate the following text: {text}"}
            ],
            model="gpt-4",
            temperature=0.2,
            max_tokens=3000,
            top_p=0.1,
            frequency_penalty=0.2,
            presence_penalty=0.1,
        )
        response_json = json.loads(chat_completion.model_dump_json(indent=2))
        content = response_json['choices'][0]['message']['content']
        return content.strip()
    except Exception as e:
        print(f"❌ Error during translation: {e}")
        return None

# 📂 Input and output directories
input_directory = "./!translator/in/"
output_directory = "./!translator/out/"

# 📁 Ensure output directory exists
if not os.path.exists(output_directory):
    os.makedirs(output_directory)

# 🧯 Check if input directory exists
if not os.path.exists(input_directory):
    print(f"❌ Error: Folder '{input_directory}' not found.")
    exit()

# 📄 Collect files and their respective translation languages
translation_choices = {}

for filename in os.listdir(input_directory):
    if filename.endswith(".txt"):
        if filename.endswith("_en.txt"):
            translation_choices[filename] = "ua"
        elif filename.endswith("_ua.txt"):
            translation_choices[filename] = "en"
        elif filename.endswith("_ru.txt"):
            print(f"🟫 File {filename} contains Russian text.")
            language_choice = input("🌍 Translate to (en) English or (ua) Ukrainian?
Enter 'en' or 'ua': ").strip().lower()
            if language_choice in ["en", "ua"]:
                translation_choices[filename] = f"ru-{language_choice}"
            else:
                print(f"⚠️ Invalid language selection for file: {filename}")
                continue
        else:
            print(f"⚠️ File {filename} does not match known suffixes for translation.")
            continue
```

```
# 🔁 Process all selected files for translation
for filename, language in translation_choices.items():
    file_path = os.path.join(input_directory, filename)
    system_prompt = get_system_prompt(language)

    # 📖 Read text from file
    with open(file_path, 'r', encoding='utf-8') as f:
        text_to_translate = f.read()

    print(f"🔄 Translating file: {filename}")

    # ✂️ Split text into smaller parts
    text_chunks = split_text_by_sentences(text_to_translate)
    translated_text = ""

    for chunk in text_chunks:
        translated_chunk = translate_text(chunk, system_prompt)
        if translated_chunk:
            translated_text += translated_chunk + "\n\n"

    if translated_text:
        # 📝 Generate output filename
        output_filename = os.path.splitext(filename)[0] + "_translated.txt"
        output_filepath = os.path.join(output_directory, output_filename)

        # 💾 Save translated text
        with open(output_filepath, 'w', encoding='utf-8') as f:
            f.write(translated_text)

        print(f"✅ Translation saved: {output_filepath}")
    else:
        print(f"❌ Failed to translate file: {filename}")

# 🎉 Notify that all translations are completed
print("🏁 All files have been successfully translated!")
```

А.8 – Python-скрипт перевірки фізичних та юридичних осіб у санкційному списку

sanctions_check.py

```
# 📑👨‍⚖️ Legal Entity and Individual Sanctions Validator

import pandas as pd

# 📂 Load data
df_individuals = pd.read_excel("./Code/!sanctions/04.03.2025 individual subjects.xlsx",
sheet_name="Individual")
df_legal = pd.read_excel("./Code/!sanctions/04.03.2025 legal subjects.xlsx",
sheet_name="Legal")

def search_individuals():
    while True:
        print("\n🔎 Individual Sanctions Search")
        surname = input("👤 Enter surname: ").strip()
        name = input("📝 Enter first name: ").strip()
        filtered = df_individuals[df_individuals['name'].str.contains(surname,
case=False, na=False)]
        filtered = filtered[filtered['name'].str.contains(name, case=False, na=False)]

        if filtered.empty:
            print("❌ No individuals found.")
        else:
            print("\n✅ Match found:")
            print(filtered[['name', 'status', 'birthdate', 'citizenship',
'sanctions_term', 'sanctions_end_date', 'decree_date']].to_string(index=False))

        next_action = input("\n🔁 What next? (1️⃣ – new search, 2️⃣ – switch to legal
entities, 3️⃣ – exit): ").strip()
        if next_action == "1":
            continue
        elif next_action == "2":
            return "switch"
        elif next_action == "3":
            return "exit"
        else:
            print("⚠️ Invalid choice. Exiting.")
            return "exit"

def search_legal():
    while True:
        print("\n🏢 Legal Entity Sanctions Search")
        keyword = input("🔍 Enter a keyword in the legal entity name: ").strip()
        matches = df_legal[df_legal['name'].str.contains(keyword, case=False, na=False)]

        if matches.empty:
            print("❌ No legal entities found.")
        elif len(matches) == 1:
            print("\n✅ One legal entity found:")
            print(matches[['name', 'status', 'sanctions_term', 'sanctions_end_date',
'decree_date']].to_string(index=False))
        else:
```

```
            print("\n📋 Multiple matches found:")
            for i, name in enumerate(matches['name'], start=1):
                print(f"{i}. {name}")
            choice = input("👉 Select the number of the desired organization: ")
            try:
                idx = int(choice) - 1
                selected = matches.iloc[idx]
                print("\n📂 Information on the selected legal entity:")
                print(selected[['name', 'status', 'sanctions_term',
'sanctions_end_date', 'decree_date']].to_string())
            except:
                print("⚠️ Invalid selection.")

        next_action = input("\n🔁 What next? (1️⃣ – new search, 2️⃣ – switch to
individuals, 3️⃣ – exit): ").strip()
        if next_action == "1":
            continue
        elif next_action == "2":
            return "switch"
        elif next_action == "3":
            return "exit"
        else:
            print("⚠️ Invalid choice. Exiting.")
            return "exit"

def main():
    current_mode = None
    print("🛡️ Welcome to the Ukrainian Sanctions Checker 🛡️\n")
    while current_mode not in ["1", "2"]:
        print("📌 Select search type:")
        print("1️⃣  Individuals")
        print("2️⃣  Legal entities")
        current_mode = input("🧭 Your choice (1 or 2): ").strip()

    while True:
        if current_mode == "1":
            result = search_individuals()
            if result == "switch":
                current_mode = "2"
            elif result == "exit":
                break
        elif current_mode == "2":
            result = search_legal()
            if result == "switch":
                current_mode = "1"
            elif result == "exit":
                break

    print("\n👋 Program terminated. Stay vigilant.")

if __name__ == "__main__":
    main()
```

Додаток Б

Громадська організація
«УКРАЇНСЬКИЙ ЦЕНТР СОЦІАЛЬНОГО ПРОЕКТУВАННЯ»

Україна, 69114, м. Запоріжжя, вул. Гудименко, 42/49
099 791 3417, www.youthplanning.org, info@youthplanning.org

Вих. № 28/05 від 28.05.2025

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Яцини Юлії Олександрівни
на тему: **«Інноваційні аналітико-статистичні технології попередження корупції в державі»,**
що подається на здобуття наукового ступеня доктора філософії
за спеціальністю 052 «Політологія»

Зважаючи на посилення викликів у сфері державного управління, пов'язаних з необхідністю адаптації антикорупційної політики до умов воєнного стану, цифровізації публічного сектора та зростаючих суспільних очікувань щодо прозорості, результати дисертаційного дослідження Юлії Олександрівни на тему «Інноваційні аналітико-статистичні технології попередження корупції в державі» мають не лише теоретичну, а й прикладну значущість. Розроблені у межах цього дослідження аналітичні моделі та програмні інструменти становлять практичний інтерес для інституцій, які впроваджують політику попередження корупції на державному та муніципальному рівнях.

Особливу увагу заслуговує авторський підхід до інституціоналізації інноваційних цифрових рішень, зокрема застосування аналітико-статистичних моделей на основі Python для автоматизованої обробки якісних даних – зокрема, стенограм фокус-групових дискусій, індивідуальних глибинних інтерв'ю та цифрових масивів громадської думки. В умовах обмежених людських та часових ресурсів, такі розробки відкривають можливості для пришвидшення циклу аналізу – від збору до інтерпретації – та водночас підвищують стандарти аналітичної обґрунтованості рішень, що приймаються у сфері доброчесного врядування.

Для ГО «Український центр соціального проєктування» зазначене дослідження є цінним джерелом знань у напрямі практичної реалізації стратегій попередження корупції з опорою на інструменти автоматизації. У цьому контексті результати дисертації відкривають перспективу для

створення цілісних систем публічного моніторингу, які базуються на принципах відкритих даних та соціальної відповідальності.

Окремо слід підкреслити цінність запропонованої у роботі класифікації аналітичних інструментів, яка дає змогу адаптувати моделі до різних рівнів управління – від центральних органів виконавчої влади до територіальних громад. Це дозволяє використовувати отримані результати не лише як теоретико-методологічне підґрунтя, а як інструментальну базу для навчання посадовців, залучення громадськості до моніторингу та розробки політик зниження корупційних ризиків.

Таким чином, дослідження має міждисциплінарну цінність і може бути використане в практичній діяльності аналітичних центрів, державних інституцій, ОГС і освітніх закладів, які займаються питаннями підвищення прозорості, формування доброчесних практик публічного управління, а також цифрової трансформації механізмів антикорупційної політики.

Вважаю за доцільне використовувати результати даного дослідження у подальшій роботі ГО «Український центр соціального проєктування».

Голова
ГО «УЦСП» Т.І. Бутченко

ГРОМАДСЬКА ОРГАНІЗАЦІЯ «УКРАЇНСЬКИЙ ЦЕНТР СОЦІАЛЬНОГО ПРОЕКТУВАННЯ» 40536796 Україна, м. Запоріжжя

Громадська організація
«СОЮЗ СОЦІАЛЬНИХ ТЕХНОЛОГІВ УКРАЇНИ»

Україна, м. Запоріжжя, 69039, вул. Нова, буд. 4
(095) 601 33 99, (067) 755 93 44, www.useu.org.ua, info@useu.org.ua

Вих. № 28/05-1 від 28 травня 2025 року

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Яцини Юлії Олександрівни
на тему: **«Інноваційні аналітико-статистичні технології попередження корупції в державі»,**
що подається на здобуття наукового ступеня доктора філософії за спеціальністю 052 Політологія

У світлі викликів, які постають перед українською державністю в умовах гібридної війни, інформаційної уразливості та спроб маніпуляції громадською думкою, особливого значення набувають інструменти, що дозволяють оперативно виявляти ризики політичної корупції, втручання у виборчі процеси та непрозорих впливів на публічну політику. У цьому контексті результати дисертаційного дослідження Юлії Олександрівни на тему «Інноваційні аналітико-статистичні технології попередження корупції в державі» становлять для ГО «Союз соціальних технологів України» не лише теоретичну цінність, а й конкретну практичну користь.

Значним досягненням автора є розробка прикладного застосунку для автоматизованої перевірки фізичних та юридичних осіб на предмет наявності у санкційних списках Ради національної безпеки і оборони України (РНБО), що оприлюднюються у формі відкритих реєстрів. Цей інструмент є особливо актуальним для представників громадянського суспільства, журналістів-розслідувачів, державних замовників та представників бізнесу, які прагнуть мінімізувати ризики співпраці з підсанкційними особами. Розробка дозволяє скоротити часові та людські витрати на первинну перевірку контрагентів, водночас забезпечуючи високий рівень точності виявлення збігів.

Не менш важливою є дослідження в сфері електоральної корупції. Авторка дослідила способи математичної ідентифікації відхилень у статистиці виборів і референдумів, які потенційно можуть свідчити про організовані маніпуляції, підкуп, мобілізацію підконтрольного електорату або спотворення

результатів волевиявлення. Запропоновані у роботі аналітичні підходи можуть бути адаптовані до роботи з офіційними масивами Центральної виборчої комісії, а також з паралельними системами громадського спостереження, що особливо важливо в умовах необхідності контролю за легітимністю виборчих процедур на всіх рівнях.

ГО «Союз соціальних технологів України» високо оцінює потенціал даних розробок у контексті формування нової архітектури цифрового громадського контролю за доброчесністю влади, прозорістю політичної конкуренції та захищеністю електорального процесу від деструктивних зовнішніх впливів. Дисертаційна робота демонструє високий рівень інтеграції прикладних знань з галузі програмної інженерії, аналізу даних та соціальної аналітики, що дозволяє рекомендувати її результати для широкого впровадження в практику роботи неурядових організацій, виборчих штабів, антикорупційних органів та органів публічної влади.

Вважаю за доцільне використовувати результати даного дослідження у подальшій роботі ГО «Союз соціальних технологів України».

Заступник голови ГО «ССТУ» Ігор Кудінов