К.П. Чехунова

ЕКОНОМІЧНИЙ ФОРЕНЗІК

ЯК БЕЗПЕКОВА ІННОВАЦІЯ ПІДПРИЄМСТВА

В УМОВАХ ЦИФРОВІЗАЦІЇ ТА РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

МОНОГРАФІЯ

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ЕКОНОМІКИ ПРОМИСЛОВОСТІ

Чехунова Катерина Павлівна

ЕКОНОМІЧНИЙ ФОРЕНЗІК ЯК БЕЗПЕКОВА ІННОВАЦІЯ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВІЗАЦІЇ ТА РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Монографія

Київ – 2026

УДК 334.7:330.341:004.8+343.37+657.4
Ч-56
JEL: D81, K42, M42, O31, O33
DOI: https://doi.org/10.37405/EFSI-2026

Рецензенти: д.е.н., проф. В. П. Антонюк,
д.е.н., проф. В. І. Ляшенко,
д.е.н., ст. досл. І. Ю. Підоричева

Рекомендовано до друку вченою радою
Інституту економіки промисловості НАН України
(протокол № 7 від 14.05.2026 року)

Чехунова К. П.

Ч 56 Економічний форензік як безпекова інновація підприємства в умовах цифровізації та розвитку технологій штучного інтелекту : монографія / НАН України, Ін-т економіки пром-сті. Київ, 2026. 175 с.

ISBN 978-617-14-0549-3

Монографію присвячено розвитку теоретико-методологічних засад використання економічного форензіку як безпекової інновації в умовах цифровізації. Об'єктом дослідження є процеси забезпечення економічної безпеки підприємства. На основі інституційної та неоінституційної теорій розкрито сутність форензіку як інструменту антикорупційної профілактики та мінімізації ризиків на межі економіки й права.

Визначено вплив технологій Четвертої промислової революції (ШІ, блокчейн, машинне навчання) на розвиток цифрового форензіку. Обґрунтовано доцільність впровадження єдиного інституційного механізму економічного форензіку, що об'єднує рівень підприємства (збір даних, аналіз ризиків) та державний рівень (інформаційна інфраструктура, законодавче регулювання). Такий підхід забезпечує прискорену ідентифікацію загроз та оптимізацію управлінських рішень.

Доведено, що економічний ефект від форензіку полягає у запобіганні фінансовим збиткам, захисті інтелектуальної власності та зниженні навантаження на правоохоронну систему. Запропоновано методичний підхід до розрахунку цього ефекту, що враховує ймовірність коректної ідентифікації ризиків. Сформульовано стратегічні напрями державної політики щодо легітимізації цифрового форензіку та координації взаємодії БЕБ, судової системи й бізнесу для зміцнення національної економічної безпеки.

Для фахівців, науковців, викладачів, аспірантів і здобувачів освіти економічних та технічних спеціальностей закладів вищої освіти, представників законодавчої й виконавчої влади, а також широкого кола читачів, яких цікавить промислова політика.

УДК 330.341.1:004.9:657.6

ISBN 978-617-14-0549-3

ЗМІСТ

ВСТУП 4

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ 9

1.1 Сутність та основні проблеми економічної безпеки підприємства 9

1.2 Ґенеза та сутність форензіку як предмета економічних досліджень 23

1.3 Цифровий форензік як безпекова інновація підприємства 36

РОЗДІЛ 2. СТАН ЕКОНОМІЧНОГО ФОРЕНЗІКУ В УКРАЇНІ ТА СВІТІ В УМОВАХ ЧЕТВЕРТОЇ ПРОМИСЛОВОЇ РЕВОЛЮЦІЇ 54

2.1 Аналіз економічної злочинності в Україні та світі 54

2.2 Аналіз стану економічної безпеки підприємств в Україні щодо використання цифрового форензіку 69

2.3 Система форензіку в контексті забезпечення економічної безпеки в Україні 80

Висновки до розділу 2 97

РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ІНСТИТУЦІЙНОГО МЕХАНІЗМУ ЕКОНОМІЧНОГО ФОРЕНЗІКУ В УКРАЇНІ 100

3.1 Концептуальні положення інституційного механізму економічного форензіку в Україні 100

3.2 Економічний ефект від упровадження інституційного механізму економічного форензіку 118

3.3 Стратегічні напрями впровадження інституційного механізму економічного форензіку на підприємствах України 137

Висновки до розділу 3 150

ВИСНОВКИ 153

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 157

ВСТУП

У сучасних умовах розвитку економічних процесів в Україні та світі все більшої актуальності набувають питання забезпечення оптимального рівня економічної безпеки підприємств, галузей і сфер економічної діяльності. Невизначеність умов діяльності, вплив різних чинників внутрішнього середовища та зовнішнього оточення створюють для підприємств певні економічні ризики та зменшують їх здатність ефективно функціонувати, а також реагувати на загрози, які можуть призвести до економічних втрат, призупинення бізнес-діяльності або банкрутства.

Одним із сучасних дієвих інструментів подолання негативного впливу економічних ризиків і недопущення загроз для функціонування підприємств є формування та використання механізму вчасного виявлення, оцінювання, аналізу, недопущення або мінімізації економічних ризиків, тобто економічного форензіку. Економічний форензік є складовою корпоративного управління, що передбачає використання методів дослідження, аналізу й експертизи для виявлення та розслідування економічних злочинів, фінансових аномалій у бізнес-процесах підприємств. Економічний форензік забезпечує підтримку необхідного і достатнього рівня економічної безпеки. Використання механізмів економічного форензіку створює можливості для підприємств організувати своєчасне виявлення, нейтралізувати або мінімізувати ризики та загрози для сталого функціонування. Одним із напрямів реалізації таких механізмів є застосування в діяльності підприємств сучасних інформаційно-комунікаційних і цифрових технологій, тобто технологій Четвертої промислової революції. Цифровізація досягла такого рівня розвитку, що стала чинником, який може неконтрольовано впливати на всі сфери діяльності підприємств, і у тому числі на їх конкурентні позиції на ринку, економічну безпеку, репутацію та прибутковість. При цьому значна кількість загроз економічній безпеці суб'єктів господарювання міститься в самих цифрових технологіях. Таким чином, актуальним у сучасній практиці організації умовно безпечної діяльності підприємств є застосування саме цифрової форми економічного форензіку – цифрового форензіку як складової корпоративного управління, що передбачає використання методів і технологій для збору, аналізу та інтерпретації цифрових даних (доказів) з

метою розслідування кіберзлочинів, комп'ютерних атак, електронного шахрайства та інших кіберпорушень. Основним призначенням цифрового форензіку є виявлення, збір та інтерпретація цифрових слідів, які можуть бути використані для підвищення рівня економічної безпеки підприємств.

Дослідженню економічної безпеки підприємств та їхньому інноваційному управлінню присвячено багато робіт вітчизняних учених (Д. Буркальцева, З. Варналій, О. Саєнко (Варналій та ін., 2011), В. Геєць, М. Кизим (Геєць та ін., 2006), В. Мунтіян (2015), О. Новікова (Новікова & Покотиленко, 2006), О. Пабат (2012), Ю. Харазішвілі (2019), І. Підоричева (2023), Н. Брюховецька, О. Чорна (Брюховецька та ін., 2024), А. Семеног (Семеног та ін., 2024), та ін.). Цю проблематику розглянуто в різних аспектах, а саме: використання цифрових технологій (В. Бакай (2020), Е. Попов, К. Семячков (Попов & Семячков, 2018), та ін.); забезпечення економічної безпеки країни (Л. Акімова (2018), Т. Корнієнко (2022) та ін.); запобігання та виявлення фінансового шахрайства (Д. Булик, В. Шикун (Шикун & Булик, 2023), О. Стецюк, В. Чубай (Стецюк & Чубай, 2023) та ін.); реалізації функцій форензіку (О. Рябчук, С. Твердун (Рябчук & Твердун, 2021), С. Тютченко (2021) та ін.); забезпечення стійкості (О. Новікова, Я. Остафійчук, Н. Азьмук, О. Панькова (Новікова та ін., 2025) та ін.). Хоча проблеми, пов’язані з форензіком та його цифровізацією, перебувають у фокусі уваги наукової спільноти (Пілецька & Колесников, 2025; Ribaux et al., 2022; Akinbi, et al., 2022; Zitzewitz, 2012; та ін.), проте недостатньо дослідженими залишаються питання аналізу та забезпечення економічної безпеки підприємств в Україні з використанням цифрового економічного форензіку. Тому дослідження аспектів використання економічного форензіку як безпекової інновації підприємства в умовах цифровізації економіки є вельми актуальним.

Метою дослідження є обґрунтування комплексу теоретичних положень і науково-методичних підходів до використання економічного форензіку як безпекової інновації підприємства в умовах цифровізації економіки.

Для досягнення зазначеної мети поставлено та вирішено такі ***завдання***:

визначено сутність і проблеми економічної безпеки підприємства;

проаналізовано ґенезу економічного форензіку та визначено його характерні особливості з позицій сучасних шкіл економічної теорії;

розкрито сутність цифрового форензіку як безпекової інновації підприємства;

визначено ризики та можливості економічного форензіку в умовах упровадження технологій Четвертої промислової революції;

проаналізовано стан економічної безпеки підприємств України щодо використання цифрового форензіку;

обґрунтовано систему форензіку в контексті забезпечення економічної безпеки в Україні;

визначено концептуальні положення інституційного механізму економічного форензіку в Україні;

обґрунтовано економічний ефект від упровадження інституційного механізму економічного форензіку;

визначено стратегічні напрями впровадження інституційного механізму економічного форензіку на підприємствах України.

Об'єкт дослідження – процеси забезпечення економічної безпеки підприємства. Предмет дослідження – теоретичні, науково-методичні та практичні засади економічного форензіку як безпекової інновації підприємства в умовах цифровізації економіки.

У роботі використано загальнонаукові та прикладні методи дослідження, у тому числі: аналізу та синтезу – для дослідження ґенези економічного форензіку з безпекових позицій, стану, сутності та проблем економічної безпеки підприємств України; індукції та дедукції – для визначення концептуальних положень інституційного механізму економічного форензіку; порівняльного та системного аналізу – для виявлення характерних особливостей економічного форензіку, обґрунтування системи форензіку в контексті забезпечення економічної безпеки в Україні та визначення стратегічних напрямів упровадження інституційного механізму економічного форензіку; економіко-математичного моделювання – для встановлення економічного ефекту від упровадження інституційного механізму економічного форензіку.

До найбільш важливих результатів, які визначають наукову новизну дослідження, належать такі:

обґрунтовано науково-методичний підхід до розрахунку економічного ефекту від упровадження інструментарію цифрового

економічного форензіку на підприємствах, що базується на скороченні потенційної шкоди від реалізації економічних ризиків за рахунок їхньої мінімізації та компенсації збитків шляхом як внутрішнього врегулювання, так і звернення до правоохоронних органів. Підхід ураховує імовірність правильної ідентифікації та мінімізації ризиків, а отже, дозволяє підвищити точність оцінки фактичного та потенційного економічного ефекту від застосування інструментів економічного форензіку;

удосконалено інституційний механізм економічного форензіку для забезпечення економічної безпеки, який поєднує внутрішній взаємозв'язок і порядок здійснення процесів та процедур, а також їх методичне, організаційне, інформаційне та правове забезпечення на рівні окремого підприємства та держави загалом. Упровадження механізму спрямоване на підвищення економічної безпеки на рівні підприємств і держави в результаті вчасного виявлення та ефективного реагування на ризики економічної безпеки в межах підприємства з використанням інструментів штучного інтелекту, машинного навчання та блокчейну, а також на вдосконалення інституціонального середовища застосування інструментів форензіку на основі даних, одержаних державою від підприємств;

удосконалено методологію організації економічного форензіку шляхом обґрунтування базової схеми процесу економічного форензіку, яка, на відміну від існуючих, містить узагальнену, концентровану та вичерпну інформацію про основні етапи здійснення економічного форензіку на підприємстві;

удосконалено каузальну схему одержання економічного ефекту від економічного форензіку на рівні підприємства та держави, а також підходи до оцінювання складності розрахунку економічного ефекту від переваг економічного форензіку на рівні підприємства (мінімізація фінансових збитків, мінімізація витрат, пов'язаних із зверненням до правоохоронних органів; дотримання законодавства; захист інтелектуальної власності; скорочення витрат на реагування на ризики; поліпшення репутації, зниження страхових премій; запобігання простоям і перебоям у діяльності; посилення довіри постачальників і партнерів; зростання продуктивності праці співробітників; конкурентні переваги) та держави (зниження навантаження на правоохоронні органи; поліпшення економічних показників підприємств за рахунок зниження збитків; збільшення податкових над-

ходжень за рахунок зменшення збитків підприємств; скорочення кількості негативних подій у сфері інтелектуальної власності та обробки персональних даних; зниження рівня економічної злочинності; загальне поліпшення економічної ситуації), що дозволяє обґрунтувати формулу розрахунку економічного ефекту від упровадження економічного форензіку;

дістали подальшого розвитку концептуальні засади формування принципів цифрового форензіку, які враховують: необхідні вимоги до експертів при отриманні цифрових доказів; умови поводження з доказами, отриманими під час цифрового форензіку; вимоги до інструментів, що використовуються для здійснення цифрового форензіку. Це дозволяє розвинути теоретичний базис методології організації та здійснення цифрового форензіку;

дістали подальшого розвитку комплекс організаційно-інституційного забезпечення цифрового економічного форензіку на підприємствах України на інституційному рівні шляхом залучення правоохоронних органів, серед яких Бюро економічної безпеки, органи статистики та групи законодавчих ініціатив, у тому числі самоврядні організації, до виконання відповідних функцій, таких як формування законодавчих засад, створення інформаційної інфраструктури, регулювання, стимулювання та координація впровадження інструментарію цифрового економічного форензіку, спрямованих на зниження навантаження на правоохоронні органи, підвищення економічної ефективності підприємств і запобігання кризовим ситуаціям;

дістали подальшого розвитку визначення терміна «економічний форензік» як дослідження передумов та наявності економічних злочинів на підприємствах із використанням методів й інструментів економічного аналізу та фінансових розслідувань з метою одержання інформації про встановлення фактів й обставин економічних злочинів для прийняття управлінських рішень та вдосконалення стану економічної безпеки. Дане визначення, на відміну від інших, характеризує економічний форензік з академічної точки зору як наукову дисципліну, об'єктом якої є економічні злочини на підприємствах і поведінка економічних злочинців, а предметом – закономірності дослідження об'єктів на основі спеціальних пізнань, трансформованих у систему методів, інструментів і засобів вирішення питань щодо виявлення економічних злочинів.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

1.1 Сутність та основні проблеми економічної безпеки підприємства

Однією з найважливіших складових економічної діяльності будь-якої компанії, спрямованої на усунення ризиків (порушення правил внутрішнього контролю, шахрайства, маніпулювання фінансовою звітністю, розкрадань, несумлінних дій контрагентів), є їх мінімізація та управління економічною безпекою бізнесу. За даними PricewaterhouseCoopers (PwC) у 2020 р. 47% вітчизняних компаній зіткнулися з розкраданням активів, хабарництвом і корупцією (PricewaterhouseCoopers, 2020).

Закономірно, що чим складніші умови функціонування бізнесу, тим вище рівень корпоративного шахрайства. Існує взаємозалежність між чинниками фінансової нестабільності, економічної кризи, банкрутствами, біржовими спекуляціями, фінансовим шахрайством й економічним спадом. Тому вкрай важливим є запобігання шахрайству як економічному злочину, оцінювання методів і підходів для виявлення шахрайських дій з метою підвищення рівня економічної безпеки.

Перш ніж розглядати концептуальні основи економічного форензіку з безпекових позицій, доцільно дослідити формування сучасних концепцій категорії «економічна безпека», розкрити значення даного поняття, загальні та відмінні аспекти в його трактуванні, використані в дослідженнях, пов'язаних з економічним форензіком.

Економічну безпеку можна трактувати як ступінь вразливості перед економічними втратами (Stiglitz et al., 2018), стан ефективного використання ресурсів для запобігання викликам і загрозам, а також забезпечення сталого функціонування підприємства (Smelik, 2020), стан існування бізнесу, в якому досягається оптимальний рівень захищеності від ризиків та загроз у всіх функціональних сферах діяльності (Onyshchenko, 2019), або можливість підтримувати адекватний дохід в умовах шоку (Edwards & Murphy, 2022).

Y. Samoilenko, I. Britchenko, I. Levchenko, P. Lošonczi, O. Bilichenko та O. Bodnar розглядають економічну безпеку як здатність інституційно-організаційної системи захищати інтереси суб'єктів господарювання на основі міжнародних і національних правових норм щодо дотримання національних традицій і цінностей господарювання (Samoilenko et al., 2022).

Ще у 1952 р. A. Wolfers у дослідженні «National Security» as an Ambiguous Symbol» трактував безпеку як «відсутність загроз набутим цінностям» (Wolfers, 1952, p. 485). Переформулювання цього визначення на «низьку ймовірність пошкодження набутих цінностей» D.A. Baldwin використав у роботі «The concept of security» (Baldwin, 1997), аргументуючи його тим, що у відповідь на загрози розробляється політика стримування, призначена для забезпечення безпеки шляхом зниження ймовірності загрози, а отже, пошкодження (втрати) цінностей. Далі автор зосереджується на визначенні специфікацій («безпека для кого?», «безпека яких цінностей?», «від яких загроз?», «обсяг безпеки?») та їхньої достатньої кількості для конкретизації категорії «безпека» в концептуальному аспекті та для наукового використання.

B. Buzan приділяє увагу розгляду категорії «безпека» з позицій економіки, а саме економічних загроз. Він зазначає, що «нормальним станом суб'єктів ринкової економіки є ризик, агресивна конкуренція та невизначеність» (Buzan, 2007, p. 124), і через цю природу небезпеки економічну безпеку важко визначити. Виходячи з позиції, що економіка є базисом матеріального життя суспільства, економічну безпеку можна вважати ключовим показником загальної безпеки держави.

У період зростання глобалізації та економічної взаємозалежності між країнами забезпечення економічної безпеки стає необхідністю. У Доповіді про розвиток людини 1994 р. економічна безпека визначена однією із семи сфер безпеки, які мають найбільший вплив на розвиток людини (продовольча, екологічна, суспільна, політична, особиста, безпека здоров'я) (UNDP, 2024). Важливість концепції економічної безпеки полягає також у тому, що вона є значущою складовою національної безпеки, оскільки гарантує незалежність країни та створює умови для стабільного розвитку.

Як свідчить аналіз досліджень з економічної безпеки, наукове осмислення концепту «економічна безпека» переважно розви-

валося з урахуванням двох аспектів: національного та індивідуального (особистого). Рідше виокремлюються категорії «міжнародна економічна безпека», «регіональна економічна безпека». Для дослідження теоретичних основ економічної безпеки підприємств більш близьким за змістом і схожим за ознаками є аналіз категорії національної економічної безпеки.

Так, індивідуальний (особистий) підхід до дослідження питань економічної безпеки передбачає розгляд економічної безпеки з позицій основних потреб та активів, необхідних людині для життя. На цій базі розроблено індекс економічної безпеки, що активно застосовується у США та країнах Європи.

У звіті Організації економічного співробітництва та розвитку (OECP) «For Good Measure. Advancing Research on Well-being Metrics Beyond GDP» (2009) J.S. Hacker визначає особисту економічну безпеку як засоби захисту людини від економічних ризиків (гарантії працевлаштування, безпеку видатків на охорону здоров'я та медичне обслуговування, пенсійне забезпечення), які зменшують ступінь вразливості перед економічними втратами та потрясіннями, включаючи безробіття, нестабільність доходів та різке падіння житлового добробуту й інших активів (Hacker, 2009).

Особисту економічну безпеку Міжнародна організація праці розглядає з позицій соціальної безпеки (визначається доступом до інфраструктури основних потреб, охорони здоров’я, освіти, житла, інформації та соціального захисту) та безпеки, пов’язаної з роботою (ILO, 2004).

Отже, детально визначається сім компонентів безпеки:

1) безпека (гарантія) доходу означає достатній фактичний та очікуваний дохід як протягом трудового життя, так і під час виходу на пенсію за віком або у зв’язку з інвалідністю;

2) безпека права (представництва) стосується індивідуальних та колективних (профспілки) прав, закріплених у законах, а також доступу осіб до установ, ведення переговорів;

3) безпека ринку праці – це широкі можливості для належної трудової діяльності, яка приносить дохід;

4) безпека (гарантія) зайнятості – захист від втрати роботи, яка приносить дохід (гарантія працевлаштування, захист від раптової втрати незалежної роботи та/або краху бізнесу, стійкі правила найму та звільнення);

5) безпека професії означає наявність ніш в організаціях і на різних ринках праці, що дозволяє працівникам будувати кар'єру (здатність працівника здійснювати діяльність відповідно до його інтересів, освіти, професійної кваліфікації та навичок);

6) безпека праці – такі умови праці в організаціях, які є безпечними та сприяють добробуту працівників (положення гігієни та безпеки праці, страхування від нещасних випадків і захворювань на виробництві, обмеження робочого часу);

7) безпека відтворення навичок являє собою доступ працівників до базової освіти та професійної підготовки для розвитку здібностей і отримання кваліфікації, необхідної для соціально та економічно цінних професій.

Визначення економічної безпеки з позицій індивіда припускає розгляд широкого кола гарантій та засобів захисту людини від економічних ризиків і загроз. Проте цей концепт економічної безпеки не враховує питання системної стійкості та стабільності, важливих критеріїв для благополуччя людини в соціокультурному контексті. Тобто мінімізація ризиків (або, з іншого боку, максимізація рівня економічної безпеки) для окремого індивіда автоматично не трансформуються в достатній рівень економічної безпеки для їх сукупності (наприклад, за галузевою чи географічною ознакою). Прикладом цього є циклічні економічні кризи, які впливають на економіку країни загалом, а зрештою – на окрему людину.

Згідно з макроекономічним (національним) підходом економічна безпека являє собою важливий чинник національної безпеки та включає широкий перелік складових. Так, до внутрішніх елементів економічної безпеки належать сировинно-ресурсна, оборонна, енергетична, фінансова, технологічна, продовольча, соціальна, демографічна, екологічна; до зовнішніх – зовнішньоекономічна (експортна та імпортна) безпека.

Ще у 1945 р. A. Hirschman стверджував, що економічна безпека означає побудову надійних економічних систем, здатних протистояти зовнішньому тиску й адаптуватися до змін за допомогою диверсифікації та гнучкості (Hirschman, 1945).

Історичні реалії повсякчас змушували зосереджувати увагу не тільки на оборонному аспекті безпеки, але й на економічних питаннях, оскільки на тлі науково-технічного прогресу країнам потрібно було захищатися від економічної залежності, зовнішніх чинни-

ків і загроз економічним інтересам, вибудовувати стратегію для забезпечення економічної стабільності.

Поступово економічні та фінансові інструменти стали, серед інших, ключовими важелями у формуванні концепту національної безпеки. Так, S.R. Ronis визначає економічну безпеку як головний елемент національної. На його думку, «без капіталу немає бізнесу; без бізнесу немає прибутку; без прибутку немає роботи. А без роботи немає податків і воєнного потенціалу» (Ronis, 2011, p. viii). Економічна безпека є центральною складовою безпеки держави, оскільки від стану економіки залежать інші сфери безпеки, а економічний потенціал у підсумку використовується для досягнення політичних цілей.

C. Dent розглядає економічну безпеку як умову захисту структурної цілісності, можливостей та інтересів політико-економічного суб'єкта в контексті зовнішніх ризиків та загроз і виокремлює вісім взаємопов'язаних та взаємозалежних критеріїв економічної безпеки: безпека поставок, безпека доступу до ринку, безпека фінансів і кредитів, безпека техніко-промислового потенціалу, безпека соціально-економічної парадигми, безпека транскордонного співтовариства, системна безпека та безпека альянсу (Dent, 2001).

R. Šimašius та R. Vilpišauskas наводять перелік характеристик економічної безпеки: стійкість економічної потужності держави та її спроможність фінансувати власні оборонні потреби; постачання країні «стратегічних товарів»; диверсифікація зовнішньої торгівлі; незалежність від домінуючих гравців міжнародної економіки; безпека від економічного шпигунства; добра макроекономічна ситуація; безпека власності; соціальна захищеність фізичних осіб; працевлаштування, визначеність робочих місць і прибутку (Šimašius & Vilpišauskas, 2005, p. 251).

I. Valeriu та A. Diamescu доводять, що економічна безпека пов'язана з усіма правилами та діями, які забезпечують правильне функціонування економіки країни, що позначається на фінансовій та економічній якості життя, а також спрямована на забезпечення належних умов для підтримки економічної діяльності в межах норм, параметрів, усунення вразливостей, протидії різноманітних атак і забезпечення стратегічного захисту (Valeriu & Diamescu, 2010). Автори торкаються питання економічної безпеки підприємств, надаючи визначення економічних злочинів із Паризької конвенції про права промислової власності: будь-які дії, які можуть викликати

плутанину щодо підприємства, продукції або промислової чи комерційної діяльності конкурента, неправдиві заяви в торгівлі, які можуть дискредитувати підприємство, продукцію чи промислову чи комерційну діяльність конкурента, фінансові ресурси, незаконно отримані шляхом економічного шахрайства.

Аналіз категорії «економічна безпека» з позицій макроекономічного та індивідуального підходів дозволив виявити суттєву різницю у трактуванні економічної безпеки прихильниками цих підходів: у рамках макроекономічного підходу термін аналізується з точки зору держави загалом, а згідно з індивідуальним – з точки зору особистості, людини. Така методологія обумовлює відмінності в розумінні економічних ризиків і загроз та, як наслідок, у визначенні мети політики, спрямованої на забезпечення економічної безпеки. У подальшому це буде враховано у процесі аналізу концепту економічної безпеки підприємства.

Значну увагу розгляду та аналізу категорії «економічна безпека підприємства» приділяють дослідники з пострадянського простору, де впродовж тривалого часу домінувала планова економіка. Відповідно, до 1991 р. питання, пов'язані з ризиками функціонування підприємства в ринкових умовах, перебували поза дослідницьким фокусом більшості вчених-економістів. Актуальність таких досліджень також обумовлена необхідністю прийняття управлінських рішень щодо зниження загроз функціонуванню підприємств, що потребує чіткого уявлення про формування та функціонування системи економічної безпеки, методів, способів й інструментів забезпечення її ефективної дії.

З метою виявлення схожих і відмінних рис у визначенні поняття «економічна безпека підприємства» доцільно проаналізувати роботи, опубліковані протягом останніх десяти років.

Так, Л. Ковальська, О. Голій та В. Голій визначають економічну безпеку підприємства як «здатність соціально-економічної системи протистояти та створити захист від дестабілізуючих чинників внутрішнього та зовнішнього середовища, забезпечуючи при цьому стійкість економічного розвитку через ефективне використання наявних і потенційних ресурсів» (Ковальська та ін., 2023, с. 129).

Л. Кургузенкова осмислює визначення поняття економічної безпеки підприємства шляхом аналізу категорій «економіка», «безпека» і «підприємство», пропонуючи розглядати економічну безпеку підприємства як «стан складної, нелінійної системи, що яв-

ляє собою відокремлений господарюючий суб'єкт при виробництві та обміні благами між людьми, у процесі якого дія зовнішніх і внутрішніх чинників не призводить до погіршення системи або неможливості її функціонування та розвитку» (Кургузенкова, 2016, с. 32).

Н. Гапак зосереджує увагу на забезпеченні захисту підприємства, визначаючи економічну безпеку підприємства як «рівень захищеності всіх видів потенціалу підприємства від внутрішніх та зовнішніх загроз, що забезпечує стабільне функціонування та ефективний розвиток і потребує управління з боку керівництва підприємства» (Гапак, 2013, с. 2).

Ю. Бондар та Т. Дорошенко розглядають економічну безпеку підприємства як «процес ефективнішого використання його виробничо-господарських ресурсів і підприємницьких здібностей, при якому забезпечується успішне та своєчасне протистояння підприємства можливим ризикам і зовнішнім загрозам, що уможливлює досягнення поставлених цілей та завдань відповідно до обраної ним стратегії розвитку» (Бондар & Дорошенко, 2022, с. 73).

Ю. Барташевська під економічною безпекою підприємства розуміє «комплекс заходів, реалізація яких дає змогу забезпечувати економічну стабільність підприємства та його розвиток за невизначеності внутрішнього і зовнішнього середовища та ризику інвестиційної діяльності» (Барташевська, 2016, с. 190).

К. Зайченко та Н. Діма визначають економічну безпеку підприємства як «систему превентивних заходів та протидії основних структурних підрозділів підприємства, відповідальних осіб у разі настання тих чи інших ризикових подій та небезпек» (Зайченко & Діма, 2021).

С. Урба та І. Івончак, проаналізувавши підходи до розгляду категорії «економічна безпека підприємництва», трактують її як «певний стан діяльності суб'єкта господарювання, за якого найбільш ефективно використовуються корпоративні ресурси, здійснюється запобігання послабленню захисту від наявних загроз чи небезпек і реалізуються поставлені цілі бізнесу в умовах посилення конкуренції та господарського ризику» (Урба & Івончак, 2018, с. 83).

О. Грибіненко та С. Шагоян надають таке визначення: «економічна безпека підприємства – ступінь захисту від негативного впливу внутрішніх і зовнішніх чинників усіх потенціалів підприємства, що дозволяють забезпечити стійку та ефективну діяльність». Разом з тим автори зазначають, що сутність поняття «містить су-

купність інструментів, які забезпечують конкурентоспроможність й ефективність підприємства і дозволяють підвищити рівень достатку персоналу підприємства» (Грибіненко & Шагоян, 2017, с. 99).

І. Колодяжна та К. Букріна розуміють економічну безпеку підприємства як «стан захищеності його важливих інтересів від внутрішніх і зовнішніх загроз для забезпечення стабільності та прогресування в сьогоденні та майбутньому» (Колодяжна & Букріна, 2019, с. 136).

І. Штулер і Д. Шевченко в результаті детального аналізу підходів до визначення поняття трактують економічну безпеку підприємства як «комплексну систему підтримання підприємства в такому стані, в якому воно забезпечує захист від внутрішніх і зовнішніх загроз, здатність адаптуватися до змін зовнішнього середовища, захищеність ланцюга створення цінності та можливість максимального досягнення основних цілей його функціонування» (Штулер & Шевченко, 2020, с. 66).

Заслуговує на увагу визначення економічної безпеки, надане О. Новіковою та Р. Покотиленком у монографії «Економічна безпека: концептуальне визначення та механізм забезпечення»: «економічна безпека – це стан захищеності економічних інтересів особи, суспільства, держави від економічних загроз та інших загроз національній безпеці, які на них впливають» (Новікова & Покотиленко, 2006, с. 247). Також автори детально розглядають питання, пов'язані з економічними інтересами та загрозами економічній безпеці.

Крім того, в Україні опубліковано цілу низку навчальних посібників з дисципліни «економічна безпека підприємства», де стисло розглянуто сутність поняття, структуру системи економічної безпеки підприємства, загрози діяльності підприємства тощо.

Огляд робіт вітчизняних дослідників свідчить про детальне розроблення категорії «економічна безпека підприємства». У табл. 1.1 наведено типологію визначень цього терміна вітчизняними науковцями, яка становить інтерес для подальшого дослідження. При цьому слід зауважити, що вимоги до оформлення результатів роботи, а також спрямованість досліджень, яка виходить за рамки мети дисертації, не дозволяють навести всі проаналізовані визначення. Так, наприклад, до розгляду не взято роботи, присвячені вузьким питанням та окремим складовим безпеки, які стосуються захисту інформації, конкурентних переваг, організаційній гнучкості тощо.

Таблиця 1.1. **Типологія визначення поняття «економічна безпека підприємства» в роботах деяких вітчизняних дослідників**

Автор, рік	Назва публікації	Ключова ознака поняття	Стан (ступінь, рівень)	Процес (забезпечення, заходи)
1	2	3	4	5
О. Новікова, Р. Покотиленко, 2006	Економічна безпека: концептуальне визначення та механізм забезпечення	Стан захищеності		
Н. Гапак, 2013	Економічна безпека підприємства: сутність, зміст та основи оцінки	Система засобів		
Л. Кургузенкова, 2016	Економічна безпека підприємства: сутність та чинники формування її відповідного рівня	Стан системи		
Ю. Барташевська, 2016	Економічна безпека підприємства: фактори впливу та шляхи забезпечення	Система заходів		
О. Грибіненко, С. Шагоян, 2017	Сутність та шляхи забезпечення економічної безпеки підприємства	Ступінь захисту		
С. Урба, І. Івончак, 2018	Економічна безпека підприємництва як об’єкт теоретико-методологічного аналізу	Стан діяльності		
І. Колодяжна, К. Букріна, 2019	Економічна безпека в системі сталого функціонування підприємства	Стан захищеності		
І. Штулер, Д. Шевченко, 2020	Сутність економічної безпеки та її система управління	Система забезпечення		
К. Зайченко, Н. Діма, 2021	Економічна безпека підприємства: сутність та роль	Система заходів		
Ю. Бондар, Т. Дорошенко, 2022	Економічна безпека підприємства як фактор забезпечення ефективності зовнішньоекономічної діяльності	Процес забезпечення		

Закінчення табл. 1.1

1	2	3	4	5
Л. Ковальська, О. Голій, В. Голій, 2023	Економічна безпека підприємства: сутність, структура та механізм забезпечення	Здатність		

Джерело: складено автором.

У рамках подальшого розвитку концепції економічної безпеки підприємств здійснено численні дослідження та надано різноманітні тлумачення, проте стандартизованого концептуального визначення категорії наразі немає. Тому концепція економічної безпеки підприємств являє собою систему уявлень про економічну безпеку та її трактувань з різних точок зору з долученням широкого кола чинників, які зумовлюють процеси управління.

Аналіз сутності та визначення поняття «економічна безпека підприємства» і систематизація одержаних результатів дозволяють виокремити дві основні характерні ознаки терміна, на які вказують автори, – стан (системний підхід) і процес (комплексний підхід). Так, прихильники системного підходу приділяють більше уваги стану, характерним рисам, властивостям системи, спроможності підприємства протидіяти загрозам і ризикам. У рамках комплексного підходу науковці аналізують безпеку з позицій комплексу заходів, що забезпечують стійке функціонування підприємства, економічну незалежність і протидію можливим загрозам та ризикам. Як об'єкт безпеки розглядається: підприємство, інтереси підприємства, потенціал підприємства, діяльність підприємства.

У рамках даного дослідження подальший аналіз буде ґрунтуватися на оцінюванні аспектів економічної безпеки з використанням як системного підходу, так і комплексного. При цьому форензік розглядатиметься як складова комплексу заходів щодо підтримки стійкого функціонування та протидії економічним загрозам і ризикам.

Аналіз досліджень, присвячених виявленню та оцінюванню економічних загроз, дозволяє виявити основні проблеми економічної безпеки підприємства: витік даних і корпоративне шахрайство. Часто витік даних відносять до загроз інформаційної безпеки підприємства, проте ця проблема нерідко призводить до економічних збитків, які важко точно оцінити: деякі дані вказують на відсутність значного негативного впливу, інші – навпаки.

Існує дослідження, у яких доведено, що витік інформації негативно впливає на фінансові показники підприємств. Так, у роботі H. Cavusoglu, B. Mishra та S. Raghunathan наведено результати аналізу впливу порушень безпеки інформаційних технологій та надання інформації з використанням ринкових оцінок. Автори зазначають, що надання підприємствами інформації про порушення інформаційної безпеки (зломи та атаки через інтернет) мали негативне значення для ринкової вартості підприємств (у середньому 2,1% ринкової вартості у перші два дні після оголошення) (Cavusoglu et el., 2004). S. Ebrahimi та K. Eshghi побудували своє дослідження на мета-аналізі робіт, присвячених оцінюванню фінансових наслідків порушень безпеки IT-систем. За результатами аналізу автори дійшли висновку про потужний взаємозв'язок між оголошеннями про порушення безпеки і падінням дохідності акцій компаній, що мали такі проблеми. Причому порушення безпеки, пов'язані з функціями, призводять до більших збитків, ніж порушення безпеки, пов'язані з даними (Ebrahimi & Eshghi, 2022). На цей взаємозв'язок впливають також тип порушення безпеки, масштаб компаній, час і країна.

Аналогічних поглядів дотримуються A. Juma'h та Y. Alnsour, стверджуючи, що витік даних впливає на загальну продуктивність компанії та сигналізує про внутрішні недоліки на підприємстві (Juma'h & Alnsour, 2020). На думку P. E. Viancourt, інвестори продовжують оцінювати витоки даних як чинник, що впливає на оцінку фірми (Viancourt, 2021). M. Ko та A. Dorantes доводять, що рентабельність активів компаній, де відбувся витік даних, знижується, незважаючи на те що продажі та операційний прибуток не зменшуються (Ko & Dorantes, 2006). S. Goel та H. Shawky доводять, що за результатами розрахунків оголошення про порушення корпоративної безпеки спричиняє збитки, які в середньому дорівнюють 1% ринкової вартості компанії (Goel & Shawky, 2009). Згідно з моделлю J. Landmann компанії, які зіткнулися з витоком даних, втратили в середньому близько 1,33% власного капіталу протягом трьох перших днів після цієї негативної події (Landmann, 2019). O.K. Tosun підкреслює, що розкриття інформації про витік даних має негативний вплив через публікації у ЗМІ та, як наслідок, впливає на бізнес у вигляді реакції фінансових ринків, що реагують зниженням надприбутків (Tosun, 2018).

Однак результати деяких досліджень свідчать про інше. Так, наприклад, K. Kannan, J. Rees, та S. Sridhar, оцінюючи вплив порушень інформаційної безпеки на фінансові показники та фондовий ринок у 1997-2003 рр., виявили, що вони не завдають суттєвих збитків компаніям у довгостроковій перспективі (незалежно від типу підприємства, сфери діяльності, виду кібератак), проте причини відсутності негативних реакцій автори віднесли до обмежень дослідження (Kannan et al., 2007). Теза, доведена понад 20 років тому, залишається актуальною і в подальшому. Наприклад, у 2014 р. глобальна платформа для електронної комерції та проведення аукціонів для купівлі та продажу більшості видів нових і вживаних товарів eBay виявила витік особистих даних 145 млн клієнтів (Wakefield, 2014). Однак цей інцидент не завадив ані зростанню вартості акцій, ані збереженню провідних позицій компаній eBay у традиційній для неї сфері діяльності.

Наразі дані є одним із найбільш важливих активів підприємств, тому загроза втрати контролю за ними стає проблемою, яка стосується всіх співробітників, власників та інших зацікавлених сторін. Для захисту інформації впроваджуються різні методи автентифікації, шифрування даних, контроль доступу користувачів, а також методи, спрямовані на мінімізацію ризиків втрати даних – навчання співробітників та протоколи роботи з даними.

Проте найпоширенішим економічним злочином є корпоративне шахрайство. Жертвою шахрайства може стати будь-хто – як внутрішні користувачі інформації (керівники компаній, акціонери, співробітники), так і зовнішні (банки, податкові установи, постачальники, покупці, інвестори, державні установи та ін.).

Наслідки шахрайства можуть бути дуже руйнівними та завдати підприємству значних фінансових та репутаційних втрат. Більшість організацій визнають вагомість таких загроз і ризиків. Іноді розкриття фактів шахрайства призводить навіть до величезних фінансових скандалів і банкрутства. Проблеми шахрайства особливо загрожують підприємствам, які не мають внутрішніх ресурсів для управління ризиками, тобто тим, які мають невеликий обіг.

У Положенні про стандарт аудиту США (SAS) № 99 «Облік шахрайства при аудиті фінансової звітності» шахрайство розглядається як «навмисна дія, спрямована на створення суттєвих викрив-

лень у фінансових звітах»[1] (Consideration of Fraud in a Financial Statement Audit, 2002). До таких дій відносять крадіжки, корупцію, хабарництво, розкрадання, «відмивання» грошей, присвоєння активів, фальсифікацію заяв, фальшиві понаднормові роботи, зловживання заробітною платою тощо.

Шахрайство, де злочинцями виступають співробітники підприємства, – це професійне шахрайство (occupational fraud), вчинене з метою досягнення особистого збагачення шляхом навмисного зловживання або неналежного (неправильного) використання ресурсів та активів підприємства, від інвестиційних афер до дрібних крадіжок (Wells, 2007, p. 20).

Ще у 1939 р. E.H. Sutherland ввів термін «white-collar crime» – злочинність «білих комірців», тобто та, що стосується бізнесу (Sutherland, 1939). Пізніше D.R. Cressey, вивчаючи питання злочинності розкрадачів, розробив класичну модель професійних шахраїв, коли довірені особи стають порушниками довіри. Вони вважають себе такими, що мають фінансову проблему (потребу), якою не можна поділитися з іншими, проте її можна таємно вирішити шляхом порушення позиції фінансової довіри та скоригувати свої уявлення про себе як про користувачів довірених коштів або майна (зловмисники вважають, що мають право користуватися активами підприємства) (Cressey, 1953).

Асоціацією сертифікованих дослідників шахрайства (ACFE) розроблено класифікатор шахрайства – «Дерево шахрайства», де основними «гілками» визначені:

(1) корупція – схема, за якою працівник зловживає своїм впливом, щоб отримати пряму чи непряму вигоду;

(2) незаконне привласнення активів – схема, за якою працівник викрадає ресурси підприємства-роботодавця або зловживає ними;

(3) шахрайство у фінансовій звітності – схема, за якою працівник навмисно викривляє або пропускає суттєву інформацію у фінансових звітах організації;

(4) крадіжка готівки в касі – схема, за якою злочинець привласнює готівку, що зберігається в касі підприємства;

[1] «an intentional act that results in a material misstatement in financial statements».

(5) крадіжка товарно-матеріальних запасів та інших активів – схема, за якою працівник викрадає безготівкові активи підприємства або зловживає ними;

(6) шахрайство з банківськими картками (скімінг) – схема, за якою вхідний платіж викрадають до того, як він буде зареєстрований у бухгалтерських книгах підприємства;

(7) шахрайство з виставленням рахунків – схема, за якою особа змушує роботодавця здійснювати оплату, надаючи рахунки-фактури на фіктивні товари чи послуги, завищені рахунки-фактури або рахунки-фактури на особисті покупки;

(8) шахрайство з нарахуванням заробітної плати – схема, за якою працівник змушує роботодавця виплачувати платіж, надаючи неправдиві дані;

(9) шахрайство з відшкодуванням витрат – схема, за якою працівник подає вимогу про відшкодування фіктивних або завищених бізнес-витрат;

(10) підробка платіжних документів – схема, за якою особа викрадає кошти роботодавця шляхом перехоплення, підробки або зміни чека чи електронного платежу, виписаного на один із банківських рахунків підприємства;

(11) підробка реєстрації виплат – схема, за якою працівник робить неправдиві записи в касовому апараті, щоб приховати шахрайське вилучення готівки (Association of Certified Fraud Examiners, 2016).

M. Rashid, A. Al-Mamun, H. Roudaki та Q. Yasser наводять три основні категорії професійного шахрайства: шахрайство у фінансовій звітності (з боку керівництва) – стосується завищення прибутків та інших активів або заниження витрат і зобов'язань з метою досягнення цільових показників ефективності; незаконне привласнення активів (шахрайство співробітників) – стосується крадіжки грошей або іншого майна працівниками; корупція (схеми закупівель і продажів, підкуп, економічне здирництво) (Rashid et al., 2022).

Проте майже половина українських респондентів або не проводять взагалі, або проводять лише неформальну комплексну перевірку підприємств з урахуванням ризиків і постійний моніторинг третіх сторін. В Україні не розповсюджені спеціальні розслідування економічних злочинів самостійно або із залученням експертів щодо оцінювання ризиків (виявлення, ранжування та усунення), внутріш-

нього контролю та моніторингу, економічного форензіку (у PwC – це послуги щодо боротьби з корупцією та шахрайством (PricewaterhouseCoopers, 2021)). Тому подальше дослідження спрямоване на аналіз методів протидії корпоративному шахрайству з акцентуванням уваги на предметі дослідження – форензіку.

1.2 Ґенеза та сутність форензіку як предмета економічних досліджень

Проблеми економічної безпеки стали стимулом для вчених-економістів до дослідження проблематики «криміналістичної» економіки, тобто використання економічних методів та інструментів для виявлення і кількісного визначення втрат від дій «економічних шахраїв». Розслідування економічних злочинів на підприємствах з метою їх виявлення, усунення та запобігання в подальшому отримало назву економічного форензіку. Також у літературі використовуються поняття «економічна криміналістика», «економіко-криміналістичний аналіз» та «економічна експертиза».

Теоретичні дослідження щодо економічного форензіку з'явилися не так давно. Потребу в цьому спричинив запит з боку підприємств і контролюючих органів щодо підвищення ефективності боротьби з корпоративним шахрайством шляхом використання можливостей економічного аналізу статистичної та фінансової звітності.

Як зазначає J.M. Connor, однією з перших спроб дослідження форензіку можна вважати роботу J.W. Jenks «The Michigan Salt Association» (1888 р.), де він за результатами аналізу діяльності трестів сформував співпадаючі цінові ряди для основних ресурсів кінцевих продуктів (кукурудза для віскі, сталь для цвяхів тощо) (Jenks, 1888). Тобто з поправкою на зміну цін на продукцію, яка відбулася через зміну ціни на вхідні ресурси, можна точно визначити, коли і наскільки сильно на ціни вплинув картель (метод розрахунку завищених цін).

У 1914 р. у Законі про повноваження Федеральної торгової комісії конгресом США було регламентовано створення Бюро економіки із спеціальними повноваженнями щодо збору даних для

проведення галузевих досліджень і судово-економічної експертизи в антимонопольних справах (Connor, 2007).

Наприкінці XIX ст. у судах активно розпочався розгляд економічних злочинів. Це було зумовлено певними чинниками. По-перше, одночасно з поступовим зниженням довіри до свідчень свідків у юриспруденції посилювалося значення наукових досліджень джерел і документів. По-друге, на початку століття зросла кількість великих підприємств, що призвело до появи монополій, де акумулювалися великі обсяги коштів та інших активів, а їх облік ускладнявся. По-третє, керівники підприємств почали викривляти дані обліку для зниження податків та отримання максимального прибутку. Тому розповсюдженим явищем стали розтрати, хабарництво, фіктивні банкрутства та шахрайство. У підсумку це призвело до інтенсивного розвитку економічної експертизи, результати якої могли б використовуватися як докази економічного злочину в суді, тобто, сучасною мовою, форензіку.

На початку XX ст. зростаюча роль економічного аналізу та використання його методів для експертизи злочинів в економічній сфері зумовила розвиток економічних досліджень для судового виробництва – судово-бухгалтерської експертизи. Проте, як буде наведено пізніше, судово-бухгалтерська експертиза не є повним аналогом економічного форензіку, хоча ці категорії мають багато спільних рис і характеристик.

У середині XX ст. спостерігалося становлення форензіку як окремої науки, про що свідчить, наприклад, виникнення у 1948 р. у США Американської академії криміналістичних наук (American Academy of Forensic Sciences), яка з 1956 р. випускає Журнал криміналістичних наук (Journal of Forensic Sciences) та наразі об'єднує представників понад 70 країн світу (American Academy of Forensic Sciences, 2024). Аналогічні процеси мали місце в Канаді, Великобританії, Австралії, а також у континентальній Європі.

Упродовж XX ст. відбувалася уніфікація обліку підприємств, формування єдиного підходу оцінювання для судової експертизи, розвивалася контрольно-ревізійна діяльність. Дістала розвитку і класифікація судової експертизи, яка охоплювала судову бухгалтерську, судову планово-фінансову, судову експертизу господарської діяльності, судову економіко-технологічну експертизу, судову експертизу ціноутворення та ін. (Іванков, 2022). Активно досліджу-

валися питання судово-бухгалтерської експертизи, змінювалися способи виявлення та боротьби з економічним шахрайством.

Як зазначає K. Dreyer у роботі «A History of Forensic Accounting», у 1960-х роках у Федеральному бюро розслідувань працювало більше 700 агентів-бухгалтерів, які спеціалізувалися на фінансових злочинах, розслідуючи справи про фінансові махінації, «відмивання» грошей та ін. (Dreyer, 2014).

На відміну від J.M. Connor, F.D. Tinari вказує на більш пізній період формування знань про економічний форензік. За його словами, галузь економічного форензіку (судово-економічної експертизи) у США вперше розвинулась у 1970-х роках, коли суди почали дозволяти експертні свідчення від постійно зростаючого кола фахівців у різноманітних дисциплінах (Tinari, 2016). Але ця позиція є недостатньо обґрунтованою в контексті історичного процесу розвитку форензіку.

У 1987 р. було створено Національну асоціацію судових економістів (пізніше – Національну асоціацію судової економіки, NAFE), що об'єднала фахівців з метою систематизації та підвищення їх якості роботи. Слід зауважити, що основним напрямом судово-економічної експертизи, наприклад у США, є вимірювання та оцінювання економічних втрат (шкоди), що включає в основному тілесні ушкодження, протиправну смерть, дискримінацію при працевлаштуванні, комерційні спори й антимонопольне законодавство (Lianos, 2012). Таким чином, поступово була створена певна спільнота експертів-економістів, які надають консультації в судових спорах.

Дослідження категорії «економічний форензік» є актуальним, оскільки це нова галузь міждисциплінарного наукового знання (економіка-право), яка вже має економічний ефект на практиці та перспективи подальшого розвитку, формуючись і пристосовуючись до засад економічної науки.

Детальний аналіз великої кількості робіт, присвячених визначенню категорії «форензік» або «економічний форензік», свідчить про те, що не існує єдиної точки зору на це відносно нове і недостатньо вивчене явище, яке до цього часу перебуває у процесі становлення.

Так, наприклад, вітчизняні науковці S. Khalymon, V. Polovnikov, O. Kravchuk, O. Marushchak та O. Strilets вказують на наявність

різниці між судово-економічною експертизою (forensic economic expertise) та судово-бухгалтерською (forensic accounting expertise); визначають економічну експертизу як дослідження фінансово-господарської діяльності суб'єкта господарювання, яке здійснюється особою зі спеціальними знаннями в галузі економіки та бухгалтерського обліку (експертом-бухгалтером) у межах чинного законодавства з метою надання висновку за колом питань, поставлених оперативними підрозділами, органами досудового розслідування чи суду (Khalymon, 2019).

О. Рябчук та С. Твердун, досліджуючи сутність поняття «форензік», трактують його як окремий вид аудиту або експертизи, метою якого є «виявлення загроз шахрайства та (або) встановлення винної особи та збір доказів за фактом порушення» (Рябчук & Твердун, 2021, с. 79).

М. Дубініна, С. Сирцева та Т. Янковська надають декілька визначень форензіку, а саме: «незалежна діяльність щодо виявлення, аналізу, врегулювання фінансових, комерційних, правових або інших питань та розроблення процедур, спрямованих на протидію всім видам внутрішньокорпоративного шахрайства; послуга щодо аналізу фінансових, правових, комерційних питань ведення бізнесу, спрямована на виявлення та зменшення ризиків виникнення шахрайства, незаконних дій та неетичної поведінки у сфері господарської діяльності, врегулювання конфліктів; вид контролю з властивими йому особливими методами, що узагальнює та поєднує бухгалтерський облік, аудит, аналіз, криміналістику, судові послуги, профайлінг, метою якого є процес виявлення фактів шахрайства, фінансових зловживань та інших злочинних дій з боку управлінського персоналу, працівників, третіх осіб, а також виявлення ризиків зловживань і розроблення системи заходів щодо їх усунення» (Дубініна та ін., 2019, с. 378).

С. Тютченко розглядає форензік як «форензік-сервіс, тобто як сервісний супровід бізнесу, спрямований на упередження виникнення ризиків корпоративного шахрайства, виявлення фактів порушення співробітниками і керівництвом компанії чинного законодавства, фальсифікації бухгалтерської та податкової звітності, випадків розкрадання або неналежного використання активів, корупції та зловживання повноваженнями, а також на оцінювання збитків від них та розроблення прийнятного механізму відшкодування шкоди і повернення активів власникам» (Тютченко, 2021).

А. Семенець пропонує введення в облікову теорію поняття «форензік-аудит», під яким «слід розуміти процес вивчення звітності та господарських операцій компанії з метою розроблення заходів щодо реагування, управління та запобігання шахрайству на підставі експертного судження про наявність фактів: порушення співробітниками і керівництвом компанії чинного законодавства; фальсифікації бухгалтерської та податкової звітності; випадків розкрадання або неналежного використання активів; корупції та зловживання повноваженнями; ризику шахрайства» (Семенець, 2019, с. 381).

К. Назарова, М. Нежива, Т. Лосіцька, В. Міняйло, Н.Новікова та О. Самборський використовують поняття форензік-аудиту, розглядаючи його як «виявлення потенційних проблем за допомогою проведення юридичного і фінансового аудиту (Назарова та ін., 2021, с. 105) або поєднання юридичного і фінансового аудиту та судово-бухгалтерської експертизи для визначення фінансових наслідків юридичних питань» (Самборський, 2023, с. 203).

О. Стецюк та В. Чубай ототожнюють поняття «форензік» та «форензік-аудит» і зазначають, що послуга фінансових розслідувань «допомагає виявити потенційні проблеми шляхом фінансового та юридичного аудиту, спрямована на запобігання вчиненню протиправних дій посадовими особами підприємства, а також на усунення зловживань службовим становищем» (Стецюк & Чубай, 2023, с. 125).

Слід відзначити, що останнім часом в Україні питання визначення сутності та методів форензіку розглядаються все активніше, обґрунтовується актуальність упровадження цього інструменту для підвищення ефективності діяльності підприємств та організацій. Проте, як свідчить вищенаведений аналіз, на сьогоднішній день не існує одностайної думки науковців щодо визначення цієї категорії.

Щодо досліджень терміна «економічний форензік» зарубіжними вченими, то «forensic economics» використовується, як правило, лише в роботах, пов’язаних з особливостями судово-економічного аналізу випадків тілесних ушкоджень і смерті осіб унаслідок протиправних дій (Ireland, 2001; Brennan & Hennessy, 2001; Fischer, 2006; Schap, 2010; Tinari, 2016) та антиконкурентної поведінки й порушення антимонопольного законодавства (Connor, 2007; Schinkel, 2008; Ewald et al., 2014). Як виключення з цього переліку можна

навести публікацію E. Zitzewitz, у якій розглянуто методи економічного форензіку та надано приклади прихованої поведінки (Zitzewitz, 2012).

Щоб далі заглибитись у визначення поняття та складових економічного форензіку, доцільно порівняти його з іншими видами перевірок бізнесу.

Аудит. На перший погляд, форензік може здаватися аудиторською перевіркою, яка теж передбачає аналіз нормативної відповідності процесів діяльності підприємства чи організації та виявлення суттєвих викривлень. Однак основною метою аудиту є підтвердження відповідності ведення обліку та звітності вимогам нормативних актів. Порядок проведення аудиту чітко регламентований на законодавчому рівні та є обов'язковим до виконання.

Аудиторська перевірка здійснюється відповідно до загального плану її проведення, в якому зазначено її обсяг та перелік контрольних заходів щодо перевірки якості роботи, також зазначаються терміни проведення робіт і виконавець. В аудиторському висновку надається інформація про суттєві викривлення в обліку та професійне судження про достовірність бухгалтерської (фінансової) звітності організації. Споживачем аудиторського висновку є зовнішні особи та контролюючі органи. Як зазначають М. Дубініна, С. Сирцева та Т. Янковська, «основною відмінністю аудиту від форензіку є те, що аудиторська діяльність регулюється на законодавчому рівні, а вимог до обов'язкового проведення форензіку законодавством не встановлено» (Дубініна та ін., 2019).

Також форензік має ширший спектр дій, і відмінність від аудиту полягає у проведенні більш масштабного дослідження. Він залучає не тільки офіційні, але і неофіційні канали інформації, додатково до первинної документації та звітності аналізуються показання контрагентів, бізнес-партнерів, співробітників й експертів. Розслідуванню підлягають усі помилки в роботі з фінансами незалежно від їхньої значущості. Звіт може бути підготовлений за запитом однієї зацікавленої особи, наприклад, власника щодо іншого партнера або керівника компанії.

Судово-бухгалтерська експертиза. Судово-бухгалтерська експертиза є поєднанням бухгалтерських і слідчих методів, що використовуються для розкриття конкретних фінансових злочинів. Вона призначається в рамках проведення цивільного, арбітражного

або кримінального судочинства для виявлення фактів протиправних дій, встановлення умов, що призвели до матеріальних збитків, визначення їх обсягу, виявлення кола осіб, причетних до вчиненого злочину.

Обсяг розслідування визначається та обмежується судом, досліджуються тільки надані на розгляд документи для розслідування конкретних проблем або операцій. Експерти не мають права спілкуватися або залучати до експертизи співробітників підприємства, які є учасниками судового процесу, проте співпрацюють з юристами та правоохоронними органами при підготовці доказів.

На відміну від судово-бухгалтерської експертизи, форензік є більш широким дослідженням, що здійснюється не тільки з метою доказу економічного злочину, але і для виявлення злочинної поведінки, сфер ризику або потенційного шахрайства. Проте може проводитися як комплексна перевірка, так і розслідування конкретних питань – залежно від завдання. Також форензік передбачає оцінювання ступеня ризику від заявлених порушень (навмисні, ненавмисні, високий або низький рівень порушень, високий або низький ризик здійснення шахрайства тощо) та, в разі потреби, надання доказів для суду. Як результат, замовник форензіку має інформацію про слабкі місця в системі внутрішнього контролю та механізми, за допомогою яких їх обходять зловмисники. Крім цього, на відміну від судово-бухгалтерської експертизи, форензік будується відповідно до принципів рівноправності сторін, регульованих нормами цивільного права. Однак у загальному розумінні судово-бухгалтерська експертиза може розглядатися як один із напрямів економічного форензіку.

Аудит шахрайства. В економічній літературі також зустрічається термін «fraud auditing» – процес виявлення й запобігання шахрайству та усунення шахрайських дій у комерційних операціях. Так, T. Singleton, A. Singleton, J. Bologna та R. Lindquist стверджують, що аудит шахрайства та економічний форензік є синонімами (Singleton et al., 2006, p. 55). Аудит шахрайства як один із напрямів економічного форензіку розглядають Д. Долбнєва (Долбнєва, 2019) та Ю. Хамига (Хамига, 2020).

Аудит шахрайства здебільшого зосереджений на створенні аудитором середовища, яке заохочує виявлення, запобігання та нейтралізацію наслідків шахрайства. Такі аудитори мають задавати тон

і стандарти етичної поведінки (ефективний корпоративний кодекс поведінки), де надано вказівки щодо конфлікту інтересів, чітке розуміння намірів управління та рівень очікувань. Також внутрішні аудитори з питань шахрайства мають дозвіл (прописаний у договорах) перевіряти записи пов'язаних сторін у процесі звичайної діяльності (особливо з постачальниками).

Аудит шахрайства може бути як внутрішнім, так і зовнішнім, із залученням аудиторських фірм та інших приватних організацій, що практикують розслідування з аудиту шахрайства. Він є частиною загального корпоративного управління і допомагає керівництву підприємства в питаннях забезпечення достатньої пильності щодо виявлення та запобігання шахрайству.

Результати аналізу літературних джерел щодо визначення сутності економічного форензіку свідчать, що термін «аудит шахрайства» зустрічається у вітчизняному науковому просторі і при дослідженні внутрішнього аудиту. Так, наприклад, О. Сметанко трактує внутрішній аудит шахрайства як діяльність внутрішніх аудиторів, спрямовану на профілактику та протидію шахрайству в системі корпоративного управління акціонерним товариством (Сметанко, 2015). Т. Павленко, О. Михайленко розглядають важливість ролі системи внутрішнього аудиту як дієвого та найбільш доступного інструменту для виявлення та попередження шахрайства (Павленко & Михайленко, 2017).

Проте саме категорія «аудит шахрайства» є найбільш наближеною за змістом до «економічного форензіку» і може вважатися як синонімом, так і напрямом форензіку – залежно від контексту питання, що розглядається.

Як зазначено вище, особлива увага при дослідженні причин економічних злочинів приділяється проблематиці розуміння поведінки (корупція, конфлікти інтересів, ступінь змови) – ці дослідницькі питання спонукають учених-економістів знаходити шляхи застосування економічної логіки для виявлення економічного злочину, його мотивів і кількісної оцінки шкоди від поведінки, яка стає предметом розгляду судів, з одного боку, та сприяти загальному розумінню поведінки економічних злочинців, яке є важливим для забезпечення ефективного функціонування економіки, – з іншого.

Таким чином, економічний форензік можна розглядати як з'єднувальну ланку між економікою та правом. Економіка пропонує

нульову гіпотезу (яка виводиться з економічної теорії), порушення якої свідчить про приховану діяльність, форензік документує порушення (або його відсутність) і надає докази потенційних альтернативних пояснень, а криміналістика збирає конкретні докази, необхідні для засудження або виправдання конкретних осіб.

Методи економічного форензіку

На думку E. Zitzewitz, незважаючи на те що питання, які стосуються економічного форензіку, відрізняються в різних підгалузях, використовувані методи економічного аналізу є досить схожими (Zitzewitz, 2012). Він наводить такі підходи до виявлення прихованої поведінки: прямі спостереження (зібрані дані, аудиторські дослідження, експерименти); порівняння двох показників однакової економічної діяльності; спостереження за результатом, який змінюється залежно від стимулів до прихованої поведінки; створення моделі чесної поведінки та перевірка даних на наявність відхилень від моделі; використання прогнозів ефективного ринку (теорія ціни).

Прямі спостереження. Прикладом прямого спостереження є дослідження B. Edelman та I. Larkin (Edelman & Larkin, 2015) про те, яким чином несприятливі соціальні порівняння по-різному спонукають працівників різних ієрархічних рівнів до обману. Автори використали оманливі самозавантаження в SSRN (Social Science Research Network – Дослідницька мережа соціальних наук), щоб показати, що працівники вищого рівня ієрархії більш схильні до обману, особливо якщо вони мали успіх у минулому. Більш успішні співробітники, які працюють довше, стикаються з більшою втратою самооцінки через негативне соціальне порівняння і більш схильні до обману у відповідь на нижчу продуктивність, ніж у колег. Дослідники підтверджують важливість порівнянь і надають докази того, що вплив негативних соціальних порівнянь відрізняється в різних робочих ієрархіях: співробітники з вищим статусом і успіхом частіше реагуватимуть на несприятливі порівняння з колегами шляхом обману, щоб зробити порівняння менш несприятливими, і це відбувається навіть після введення широкого набору засобів контролю, демографічних показників та інституційної культури. Даний висновок має велике практичне і теоретичне значення як для науковців, так і для керівників організацій.

Порівняння двох показників. C. Snyder та O. Zidar, використовуючи дані щодо публікацій у резюме економістів із 25 провідних

економічних факультетів США, довели наявність навмисного приховування інформації, спричиненого тим, що політика журналу «Американський економічний огляд» (American Economic Review) щодо публікації нерецензованих статей у тому ж обсязі, що й рецензованих, надає економістам можливість доповнювати свої резюме та видавати статті й матеріали за рецензовані (Snyder & Zidar, 2011).

Автори шляхом порівняння даних резюме та змісту журналу «Американський економічний огляд» підтвердили гіпотезу про те, що економісти з більшою кількістю статей і матеріалів схильні до додавання нерецензованих статей до переліку у заплутаний спосіб, коли їх важко відрізнити від рецензованих. Також вони виконали аналіз різниці у відмінностях поведінки цитування як на рівні демографічних груп, так і окремих осіб, який засвідчив, що економісти, які частіше цитують статті та матеріали, як правило, є тими, хто більше обманює, коли ключовим чинником виступає судження про престижність журналу та просування по службі.

Спостереження за результатом, який змінюється залежно від стимулів до прихованої поведінки. R. Di Tella та E. Schargrodsky, вивчаючи вартість товарів і матеріалів, сплачену приватним постачальникам державними лікарнями в Буенос-Айресі у 1996-1997 рр., звернули увагу на те, що під час перших шести місяців боротьби з корупцією (проведення аудиту державних закупівель) простежується спад цін на 15%, після чого ціни поступово, проте дуже повільно, починають підвищуватися (Di Tella & Schargrodsky, 2003).

Автори зазначають, що вища заробітна плата, яка сплачувалася до проведення аудиту, не відіграє жодної ролі у формуванні цін та товари та матеріали для лікарень, проте має чітко визначений негативний вплив на останньому етапі аудиту.

Розроблення моделі чесної поведінки та перевірка даних на наявність відхилень від моделі. У деяких дослідженнях економічного форензіку, де використовуються різниці в стимулах, часто вихідним припущенням є те, що стимули до прихованої поведінки не корелюються з іншими чинниками та можуть впливати на змінні результату. Тоді будується проста модель взаємодії агентів за відсутності прихованої поведінки, і таку поведінку можна виявити шляхом пошуку відхилень, або використовуються статистичні моделі, у яких прихована поведінка виявляється шляхом пошуку викидів.

R. Porter та J. Zona досліджують особливу форму змови на аукціонах державних закупівель на початку 1980-х років при будівництві автомагістралі на Лонг-Айленді (Porter & Zona, 1993). Автори виявили наявність «додаткових торгів», коли група учасників не домовляється про переможця аукціону (схема ротації ставок, за якої лише один учасник групи робить ставку), а декілька членів групи подають фіктивні вищі ставки, щоб зробити виграшну ставку конкурентоспроможною (участь у ставках на більшість вакансій). Їхній метод передбачає оцінку логістичної моделі для прогнозування учасника з найнижчою ціною на аукціоні, оцінку логістичної регресії для прогнозування рейтингу всіх учасників, а потім перевірку рівності коефіцієнтів у двох моделях. Основним припущенням є те, що фірми-учасниці аукціону повинні використовувати змішані стратегії, а отже, їхні ставки мають бути непередбачуваними залежно від спостережуваних змінних. Якщо на аукціонах, які вони виграють, поведінка фірм у торгах по-різному пов'язана з їх витратами, ніж на аукціонах, які вони не виграють, то це вказує на таємну схему.

Використання прогнозів ефективного ринку (теорія ціни). Прикладом застосування досліджень ефективності фінансового ринку в рамках економічного форензіку є робота B. Knight, де автор використав аналіз цін на активи для вимірювання очікувань інвесторів щодо прихованої поведінки, а також очікувань інвесторів, чи отримають компанії вигоду від того, що Дж. Буш здобув перемогу на виборах 2000 р. (Knight, 206). Дослідження було сфокусовано на тестуванні впливу державної політики на ринок акцій із використанням двох джерел даних: доходи від прямих інвестицій та перспективи виборів кандидатів (ціни на політичні ф'ючерсні контракти). Після оголошення стали з'являтися повідомлення про зростання цін на акції компаній, які віддали перевагу в рамках передвиборчої платформи Дж. Бушу (Pfizer – на 4,1%, Exxon – на 1,3, Philip Morris – на 6,5%), а компанії, які підтримували А. Гора, оцінювались на 6% менше. Отже, автор виявив існування ринку цінних паперів, що залежить від виборів президента США.

Складність розгляду категорії економічного форензіку з академічної точки зору полягає в тому, що в рамках академічної науки (в даному випадку – економіки) розробляються та застосовуються методи й інструменти для здобуття нових знань, а форензік (як інструмент криміналістики) передбачає використання методів й

інструментів економіки для прийняття правових рішень. Тому майже всі дослідження щодо економічного форензіку переходять у практичну площину, оскільки економічний аналіз вважається форензіком тільки тоді, коли він виконується з метою отримання інформації, яка може (проте не обов'язково) стати підставою для прийняття правових (юридичних) рішень. Саме це відрізняє форензік від інших видів перевірок діяльності підприємств. Навіть матеріали, що публікуються в журналі Національної асоціації криміналістичної економіки США (The National Association of Forensic Economics), мають практичний характер та становлять основу для багатьох судово-економічних висновків і часто використовуються в судових засіданнях.

Таким чином, економічний форензік (або просто форензік) насамперед має практичний характер, проте як наукова дисципліна (економічний форензік – це сукупність економічних методів, які використовується для визначення фактів у справі на будь-якому етапі правозастосування) він генерує знання про досліджуваний предмет і методи, підвищуючи доказову цінність економічного аналізу.

Форензік можна розглядати з позицій інституційної школи економічної теорії (Coase, 1992; North, 1992; Williamson, 1998; Furubotn& Richter, 1997), тобто через процеси впливу на рішення економічних агентів і врахування норм та правил поведінки. Проте розвиток цієї позиції потребує окремого дослідження через відсутність наукових доробків у даному напрямі. Доцільно навести деякі міркування щодо цього, на які підштовхнули напрацювання R. Lajeunesse (Lajeunesse, 2015) та F. Tinari (Tinari, 2001). По-перше, форензік як специфічний метод економічного аналізу не відповідає формалізму (формальній системі логічних зв'язків) неокласичної школи; дослідження, виконувані експертами з форензіку, потребують більш цілісного аналітичного підходу. По-друге, методи індукції та дедукції є менш поширеними, ніж методи прямого спостереження, опису й емпіричних перевірок. По-третє, у рамках форензіку вивчається поведінка економічного злочинця як «зламаний процес» у системі соціальних відносин й інститутів, який може еволюціонувати залежно від умов, що змінюються (наприклад, моделей відносин, зміни технологій).

Таким чином, відповідно до цілей дисертації обґрунтованим є таке визначення: *економічний форензік – це дослідження перед-*

умов та наявності економічних злочинів на підприємствах із використанням методів й інструментів економічного аналізу (економіка) та фінансових розслідувань (право).

До сфер економічного форензіку належать фінансовий аналіз, економічний аналіз (мікро-, макро-), аудит обліку, аналіз ринків, кримінальна психологія та фінансові розслідування.

Економічний форензік спрямований на *одержання інформації (доказів загроз, наявності економічного злочину або злочинної поведінки), яка може стати підставою для прийняття правових (юридичних) рішень і використовуватися для вдосконалення методів запобігання вчиненню протиправних дій на підприємстві.*

Сфера компетенцій експертів з економічного форензіку: від упередження виникнення ризиків та виявлення загроз протиправної поведінки до розкриття фактів корпоративного шахрайства, неправомірних дій співробітників, корупції, кількісного визначення завданої шкоди.

Об'єктом дослідження форензіку є економічні злочини на підприємствах і поведінка економічних злочинців. Під економічним злочином розуміються дії або бездіяльність осіб (фізичних та/або юридичних) з метою отримання особистої вигоди (забезпечення вигодою інших осіб) на шкоду інтересам підприємства, заподіяння матеріальної (нематеріальної) шкоди. Наприклад, корпоративне шахрайство, присвоєння або розкрадання, зловживання повноваженнями, комерційний підкуп, корупція, фіктивне банкрутство тощо.

Предмет економічного форензіку становлять закономірності дослідження об'єктів на основі спеціальних пізнань, трансформованих у систему методів, інструментів і засобів вирішення питань щодо виявлення економічних злочинів та протидії їм шляхом підвищення рівня економічної безпеки. До них належать: пошук ознак економічного злочину, доказ економічних злочинів і загроз, вивчення їхніх слідів (шляхом аналізу первинної документації, показань контрагентів, бізнес-партнерів, співробітників і експертів, оцінювання ризиків корпоративного шахрайства, аналізу доказів, спостереження, аналітичних процедур, кількісного оцінювання фінансових втрат, розроблення пропозицій щодо попередження та запобігання економічним злочинам).

Слід відзначити, що наведені визначення є неостаточними, оскільки комплексне дослідження з економічного форензіку розпочато не так давно, а розвиток світової економіки та міжнародних ринків в умовах Четвертої промислової революції, удосконалення фінансових інструментів, а також вразливість економіки з точки зору шахрайства, в тому числі в цифровій сфері, корупції та зловживань потребують нових підходів до підвищення ефективності економічної безпеки на підприємствах. Одним із таких напрямів є цифровий форензік.

1.3 Цифровий форензік як безпекова інновація підприємства

Унаслідок всеохоплюючого проникнення цифрових технологій у діяльність підприємств економічні злочини значною мірою трансформувалися. З'явилися інші форми злочинності, які надають нові шляхи для злочинів, такі як крадіжка особистих даних, електронних транзакцій та коштів, розповсюдження нових видів комп'ютерних вірусів. За допомогою цифрових технологій вчиняються крадіжки, розтрати, саботажі, шахрайство, хабарництво, шпигунство, змови, вимагання тощо.

На сьогодні не існує підприємств та організацій, які не використовують комп'ютери та ІКТ у своїй діяльності, – вони стали невід'ємною та ключовою характеристикою бізнесу. По суті, комп'ютери є електронним сховищем критично важливих для підприємства даних, які стосуються матеріальних і нематеріальних активів, включаючи запаси продукції на складах, товарів, що перебувають у процесі виробництва, інформації про контракти, продажі, виставлені рахунки, сплачені податки тощо. Усе це стає метою економічних злочинів. Разом із тим швидкість вчинення електронних злочинних дій скоротилася до наносекунд, і географічні обмеження вже не перешкоджають цьому.

Експерти з комп'ютерного форензіку (Computer Forensics) враховують дані аспекти при розгляді економічних злочинів, пов'язаних із використанням цифрових технологій. Як зазначає I. Shakeel, комп'ютерний форензік – це система методів і процедур збору доказів із комп'ютерного обладнання та інших пристроїв

зберігання цифрових даних, які можуть бути представлені в суді (Shakeel, 2015). Основними завданнями експертів із комп'ютерної криміналістики є відновлення даних, моніторинг електронних журналів та збір даних (з пристроїв, що вийшли з ладу або пошкоджені).

Цифровий форензік деякий час був синонімом комп'ютерного форензіку, проте сфера його дії поступово розширювалася, і наразі цифровий форензік охоплює дослідження всіх пристроїв, що зберігають цифрові дані, та належить до галузі кібербезпеки, орієнтованої на відновлення і розслідування матеріалів, виявлених у цифрових пристроях або хмарних сервісах. Оскільки діяльність людини все більшою мірою залежить від комп'ютерних систем і хмарних обчислень, цифровий форензік стає важливим аспектом для підприємств, тому що передбачає ідентифікацією та вивчення цифрових доказів із використанням науково прийнятих і перевірених на практиці методів. Тобто основною метою цифрового форензіку є виявлення, захист, збір, аналіз і представлення правових та електронних доказів, які розглядаються як потенціал для розкриття злочину (Kim & Kim, 2010).

У рамках даного дослідження доцільно розглянути історичний аспект формування та розвитку цифрового форензіку.

Робота Д. Паркера «Злочин через комп'ютер» (1976 р.) є одним із перших доробків про використання цифрової інформації для розслідування та переслідування злочинів, скоєних за допомогою комп'ютера. Оскільки комп'ютери здебільшого не були підключені до зовнішнього світу у вигляді мережі Інтернет, яка ще не була запущена, системні адміністратори відповідали за безпеку тільки власних систем. Тому автор розглядає випадки шахрайської поведінки співробітників компаній та проведення системного аудиту для забезпечення ефективності й точності обробки даних (першого систематичного підходу до комп'ютерної безпеки). Побічним продуктом таких аудитів було те, що інформація, зібрана під час перевірок, могла бути використана для розслідування протиправних дій (Parker, 1976).

Згодом Міністерством оборони США, Службою внутрішніх доходів (IRS) і Федеральним бюро розслідувань (ФБР) було створено спеціальні групи добровільних агентів правоохоронних органів, які пройшли підготовку з вивчення та опанування комп'ютер-

них систем. Співпрацюючи із системними адміністраторами компаній, такі слідчі допомагали отримувати інформацію з мейнфреймів (збережені дані та журнали доступу). Проте державні органи ще довгий час скептично сприймали потенціал комп'ютерів як інструменту злодіїв.

У 1978 р. було ухвалено «Закон Флориди про комп'ютерні злочини» (Musca Law, 2023), який містив положення про несанкціоновану зміну або видалення даних у комп'ютерній системі, а також про пошкодження комп'ютерного обладнання, включаючи мережі. Максимальне покарання за один злочин становило до 5 років тюремного ув'язнення та штрафи. У 1983 р. аналогічний закон було ухвалено в Канаді (Government of Canada Publications, 2024), у 1989 р. – в Австралії (Hughes, 1991), у 1990 р. – у Великій Британії (Computer Misuse Act, 1990). У 1980-90-х роках почали з'являтися спеціалізовані групи та об'єднання для проведення аналізу та розслідування кіберзлочинів (Tunggal, 2024).

P. Collier та B. Spaul, досліджуючи діяльність правоохоронних органів і консалтингових компаній щодо дотримання законодавства про неправомірне використання комп'ютерів, зазначають, що для підвищення її ефективності доцільним є об'єднання юридичних, судових і комп'ютерних навичок. Для нової дисципліни запропоновано термін «комп'ютерна криміналістика» (Collier & Spaul, 1992).

У 2000-х роках мобільні телефони стали вже не просто пристроями зв'язку, а перетворилися на смартфони, набуваючи можливостей комп'ютерів. Це створило нові можливості як для кіберзлочинців, так і для інституцій із протидії їх діяльності. Відповідно, швидке зростання кіберзлочинності в ці роки стало поштовхом для розроблення стандартів цифрового форензіку. Так, у 2001 р. було опубліковано «Загальну методологію тестування інструментів комп'ютерної експертизи. Проект тестування засобів комп'ютерного форензіку» (NIST, 2024), у 2003 р. – «Визначення інструментів цифрової криміналістичної експертизи та аналізу» (Carrier, 2003), у 2006 р. – «Онтологію кіберфорензіку: створення нового підходу до вивчення кіберфорензіку» (Brinson et al., 2006). З'являються роботи, присвячені формуванню нової навчальної дисципліни (Irons et al., 2009).

У 2004 р. набула чинності Конвенція про кіберзлочинність (Будапештська конвенція), перший міжнародний договір, де містяться керівні принципи розвитку національного законодавства в напрямі боротьби з інтернет- та комп'ютерною злочинністю (кіберзлочинністю), удосконалення методів розслідування та розширення співробітництва між країнами (Convention on Cybercrime, 2004).

Проте вже у 2010 р. S. Garfinkel відзначає, що «золоте століття комп'ютерного форензіку швидко добігає кінця»: дослідження щодо форензіку будуть дедалі відставати від ринку, інструменти ставатимуть усе більш застарілими через збільшення кількості цифрових носіїв, розповсюдження шифрування, зростаючу різноманітність операційних систем і форматів файлів (Garfinkel, 2010). Ці застереження не справдилися. Замість «добігання кінця» відбувалася чергова трансформація форензіку відповідно до технологічних викликів.

Для забезпечення ефективного управління бізнес-операціями в результаті переходу на цифрові документи формується попит на нову цифровізацію форензіку. Співробітники стають більш компетентними в цифрових технологіях, вони схильні не лише працювати в цифровому просторі, але і займатися корпоративним шахрайством. Для дієвого захисту бізнесу в умовах подальшої цифровізації бізнес-ландшафту керівники підприємств все частіше користуються послугами експертів із цифрового форензіку, які можуть допомогти виявити цифрові докази в межах відповідного розслідування.

Отже, для підприємств та організацій цифровий форензік може стати важливим інструментом розслідування широкого кола питань, таких як:

витік даних – за допомогою цифрового форензіку можна визначити джерело витоку викрадених даних і відповідальних осіб;

кіберзлочинність – збір доказів злому, шахрайства, крадіжок інтелектуальної власності;

неправомірні дії працівників – цифровий форензік може використовуватися для розслідування крадіжок, шахрайства та переслідування;

крадіжка інтелектуальної власності – розслідування несанкціонованого копіювання або розповсюдження комерційної таємниці.

Крім того, цифровий форензік може використовуватися для допомоги підприємствам у дотриманні правил, що регулюють конфіденційність і безпеку даних – проведення перевірок систем і даних підприємств, надання інформації по передові методи забезпечення безпеки (Diaz, 2023).

Як свідчить дослідження, виконане E. Yeboah-Boateng, всі відстежені кінцеві користувачі (менеджери та інші співробітники) порушували політику користування ІКТ на підприємстві, що викликає серйозне занепокоєння в керівників установ, які зацікавлені в тому, щоб не стати кібержертвами (Yeboah-Boateng, 2015). Статистика вказує на негативну динаміку. Якщо у 2012 р. до 40% порушень, пов'язаних із даними, пояснювалося недбалістю кінцевих користувачів (Ponemon Institute, 2012), то у 2020 р. цей показник сягнув 88% (Sjouwerman, 2020), у 2024 р. – 95% (FORTRA, 2024). Це відбулося через різні причини – від слабких паролів, неправильної обробки даних до системних збоїв і втрати ноутбуків й інших мобільних пристроїв.

Навіть сьогодні більшість користувачів не мають належної освіти і досі практикують поведінку, яка наражає підприємство на ризик. Поінформованість про кібербезпеку має стати пріоритетом, оскільки кіберзагрози підприємствам можуть призвести навіть до припинення діяльності чи закриття бізнесу.

У Звіті IBM зазначено, що зловмисники можуть розглядати підприємства як сукупність особистостей. Це дає їм можливість обирати своєю метою конкретну людину, а не корпоративну інфраструктуру чи програму. Крім того, обрана жертва кіберзлочину також може бути ціллю як окрема особа, а не лише як співробітник. Тобто особиста діяльність і життя працівників можуть бути використані для завдання економічної шкоди підприємству (IBM Security Systems, 2012, p. 77).

Разом із тим слід ураховувати, що в сучасних умовах будь-яка людська діяльність залишає цифровий слід, і кожен злочин також має свій цифровий слід, який і є предметом дослідження експертів із цифрового форензіку.

Інформація, виявлена у процесі форензіку, стає доказом лише тоді, коли проходить ретельну перевірку на допустимість. Одним із найважливіших аспектів обґрунтування допустимості є доказ того, що інформацію було отримано та оброблено належним чином, а отже, одержаним результатам можна довіряти.

У контексті поглиблення цифровізації докази набувають цифрової форми. Цифрові докази належать до будь-якого типу даних, що зберігаються на цифровому пристрої (наприклад на комп'ютері або мобільному телефоні), та можуть бути використані як докази при розслідуванні або у процесі судової справи. Це будь-яка форма електронних даних, документ, транзакція (фінансовий запис придбання товарів, послуг, оплата рахунків, зняття або внесення грошей), аудіо- або відеофайл.

У статті P. Reedy «Огляд Інтерполу щодо цифрових доказів за 2019-2022 роки» («Interpol review of digital evidence for 2019-2022») використано більше 250 посилань, що свідчать про актуальність досліджень щодо дешифрування, штучного інтелекту, машинного навчання, Darknet, криптовалюти (Reedy, 2023).

У процесі аналізу різноманітних джерел для збору доказів експерти з цифрового форензіку розробляють певну програму розслідування фінансових та інших економічних злочинів, яка включає прямі інтерв'ю, спостереження, інвентаризацію тощо.

Існують прямі та непрямі докази. Прямі докази встановлюють факт, а непрямі можуть свідчити про його наявність. E. Casey в роботі «Цифрові докази та комп'ютерні злочини: криміналістика, комп'ютери та інтернет» («Digital evidence and computer crime: forensic science, computers and the internet») обґрунтовує неспроможність позиції, згідно з якою цифровий доказ не може бути прямим через його відокремленість від подій, які він представляє (Casey, 2011). Автор стверджує, що цифрові докази можна використовувати для підтвердження фактів. Якщо, наприклад, піддається сумніву надійність комп'ютерної системи, то показ належного функціонування цієї конкретної системи є прямим доказом її надійності, тоді як показ належного функціонування ідентичної системи – непрямим. Аналогічно запис комп'ютера є прямим доказом того, що певний обліковий запис використовувався для входу в систему в певний час, і водночас непрямим доказом того, що особа, яка володіє обліковим записом, несе відповідальність. Інші джерела цифрових доказів, такі як створення журналів безпеки, можуть вказувати на те, що власник облікового запису був єдиною особою, яка перебувала поблизу комп'ютера під час входу (Casey, 2011, p. 72). Прямі докази вважаються більш цінними, оскільки вони безпосередньо

одержані експертами (наприклад, при огляді інформації на комп'ютері підозрюваного або при аналізі транзакцій).

Експерти з цифрового форензіку, як правило, працюють відповідно до певної програми розслідування цифрових економічних злочинів для одержання достатніх і відповідних доказів, пов'язаних із випадками шахрайства. Вони використовують різні джерела для збору таких доказів: прямі інтерв'ю з підозрюваними, інтерв'ю з колегами підозрюваних, спостереження за поведінкою конкретних співробітників чи підозрюваних, вибудовування схеми потенційного економічного злочину (транзакцій та системи відносин), збір підтвердження третіх сторін, фізичні перевірки та підрахунки фізичних активів тощо. Усі докази, зібрані з різних джерел і за допомогою різних методів, мають бути відповідним чином зафіксовані. Докази мають узгоджуватися між собою, тому подання та запис доказів є важливими частинами процесу розслідування.

Стала практика застосування цифрового форензіку та її осмислення формують відповідну методологію. Як правило, спроби описати процедуру будь-якого цифрового форензіку зводяться до аналізу програмних продуктів, які були використані для пошуку цифрових доказів. Такі дослідження є унікальними і не можуть бути використані іншими експертами через відсутність формалізованого загального підходу. Проте в них є спільні риси – це кроки (етапи), з яких складається перевірка. Найпоширеніші з них описав E. Casey, намагаючись створити інструкцію щодо здійснення цифрового форензіку будь-якого напряму: підготовка (розроблення плану дій), опитування та ідентифікація, збереження цифрових доказів, експертиза та аналіз, підготовка звіту (Casey, 2011, p. 189-190).

На сьогодні існує кілька моделей, що описують процес цифрового форензіку. Слід зазначити, що це невичерпний перелік, і з часом він поповнюватиметься. Для аналізу взято кілька моделей у хронологічній послідовності, що мають характерні відмінності.

У 1995 р. M. Pollitt запропонував методологію дослідження комп'ютерного форензіку, яка складається з 4 окремих етапів: одержання (доказів); ідентифікація (перетворення цифрових доказів на формат, прийнятний для аналізу); оцінювання (цифрових доказів із позицій причетності до злочину); надання (інформації зацікавленій стороні) (Pollitt, 1995).

У колективному дослідженні, виконаному для Конференції цифрових криміналістичних досліджень, запропоновано процес цифрового форензіку загального призначення, який складається з 6 фаз (A Road Map for Digital Forensic Research, 2001). Модель DFRWS (Digital Forensic Research Workshop) включає такі етапи: ідентифікація (виявлення профілю, моніторинг системи); збереження та захист доказів; збір (доказів із застосуванням різних методів відновлення); експертиза (відстеження та перевірка доказів, відновлення прихованих/зашифрованих даних); аналіз (статистичний, економічний); документування (звіт).

У 2004 р. B. Carrier та E. Spafford спробували об'єднати різні доступні процеси дослідження цифрового форензіку в одну інтегровану модель. Також вони ввели поняття «цифрове місце злочину» – віртуальне середовище, створене програмним і апаратним забезпеченням, де існують цифрові докази злочину чи інциденту (Carrier & Spafford, 2004). Автори пропонують такі етапи дослідження: готовності (до операцій з тестуванням цифрових інструментів, що будуть використані при перевірці, та налаштуванням обладнання); розгортання (реалізація механізму виявлення та підтвердження інциденту); фізичного розслідування місця злочину (збір і аналіз речових доказів); цифрового розслідування місця злочину (збір та аналіз цифрових доказів); презентації (надання матеріалів керівництву підприємства або суду).

Модель процесу польового сортування кіберфорензіку (CFFTPM), розроблена в 2006 р. M. Rogers, J. Goldman, R. Mislan, T. Wedge, S. Debrota (Rogers et al., 2006), має на меті реалізацію підходу до здійснення цифрового форензіку для забезпечення ідентифікації, аналізу та інтерпретації цифрових доказів за короткий проміжок часу. CFFTPM складається з 6 основних етапів, які поділяються на 6 підетапів. Починається перевірка з типового етапу планування; далі – сортування (докази ідентифікуються та ранжуються за важливістю чи пріоритетністю); аналіз активності профілю користувача (пов'язування доказів із підозрюваним у шахрайстві); етап «хронологічної шкали» (визначення послідовності ймовірних злочинних дій); «етап інтернету» (дослідження доказів, пов'язаних з інтернетом); етап «конкретних справ» (фокусований огляд доказів з урахуванням особливостей справи).

У 2009 р. S. Perumal запропонував ще одну модель цифрового форензіку, яка складається з 7 етапів: планування; ідентифікація; розвідка; зберігання доказів; аналіз; надання доказів і захист; архівне зберігання (Perumal, 2009). Доцільно розглянути ті етапи, які зустрічаються вперше. На етапі розвідки виконується перевірка обладнання та програмного забезпечення «в роботі» без відключення від мережі та серверів – сьогодні підприємства мають великі комп'ютерні мережі, а також можуть мати віддалені місця роботи, великі сховища на серверах, що унеможливлює створення зображення цифрового доказу. Етап надання доказів і захисту забезпечує підтвердження обґрунтованості перевірки висновками. На етапі архівного зберігання зберігатимуться всі докази, які, можливо, знадобляться в найближчому майбутньому як довідкові та для навчальних цілей.

У 2011 р. Y. Yusoff, R. Ismail та Z. Hassan проаналізували існуючі на той час моделі та запропонували загальну модель комп'ютерного форензіку, відому як GCFIM (Yusoff et al., 2011), яка містить 5 етапів: попередній процес (стосується всіх робіт, які необхідно виконати до фактичного розслідування та офіційного збору даних); збір та збереження даних; аналіз (отриманих даних з метою ідентифікації джерел злочину та виявлення відповідальних осіб); презентація (висновки документуються та надаються зацікавленим особам); постпроцес (повернення цифрових доказів, оцінювання здійсненого форензіку для вдосконалення майбутніх перевірок).

На основі попередніх моделей у 2013 р. було запропоновано порівняльну модель цифрового форензіку (Comparative Digital Forensic Model), що складається з 5 етапів: «основа» (розроблення систематичного плану перевірки, тестування інфраструктури); збір і збереження (ідентифікація цифрових доказів і всіх джерел даних); перевірка й аналіз (вилучення даних, генерація доказів, запис висновків); презентація та документація (звіт); обґрунтування та розповсюдження (закриття перевірки) (Kalbande & Jain, 2013).

У 2017 р. R. Montasari представив модель стандартизованого процесу цифрового форензіку (SDAPM) (Montasari, 2017). Це була спроба формування єдиного підходу до збору даних у цифровому форензіку. Він зробив декомпозицію процесу збору даних у формі алгоритму. Крім того, автор розробив десять принципів для збору надійних цифрових доказів, які запропонував використовувати як стандартні вимоги:

1. важливість взаємодії цифрового та фізичного дослідження (для збереження ланцюга контролю, цілісності цифрових доказів та їх захисту від пошкодження; забезпечення ефективної перевірки);

2. отримання дозволу на проведення перевірки від власників цифрових технологій і дотримання політики конфіденційності;

3. оцінювання ризику перед етапом збору;

4. безпека зберігання цифрових і речових доказів (ізоляція системи від мережі, виявлення підозрілих процесів, створення резервної копії зображення системи);

5. ведення детальної документації (повний шлях імен файлів, файлових систем, вхідні та вихідні адреси тощо);

6. відстеження всіх дій, пов'язаних із цифровими доказами (контрольний слід);

7. контроль обмеженого доступу (до отримання та перегляду даних);

8. збереження ланцюга відповідальності (при отриманні даних, наданні копій іншим експертам та ін.);

9. ефективне управління процесом цифрового форензіку;

10. управління інформацією у процесі форензіку між зацікавленими сторонами (обмін даними, захист цілісності інформації та конфіденційності доказів).

Сьогодні SDAPM є найбільш систематичним і детальним процесом збору цифрових даних.

У 2022 р. G. Horsman та N. Sunde розробили модель робочого процесу цифрового форензіку (DFWM) і представили новий підхід до структурування й визначення процедур і завдань, пов'язаних із процесом цифрового форензіку. DFWM містить 11 етапів робочого процесу, визначених з урахуванням власного досвіду, існуючих моделей та найкращих практик. Кожен етап описує відповідні фізичні завдання, пов'язані когнітивні та дослідницькі завдання (оцінки та рішення), ризики, обумовлені будь-якими процедурами (Horsman & Sunde, 2022):

1. Аналіз вимог клієнта та планування форензіку (оцінювання стратегії перевірки, вимог клієнта, визначення потенціалу обладнання та програмного забезпечення для ефективної роботи).

2. Ідентифікація, обробка, збереження та збір даних (встановлення пріоритетів при ідентифікації пристроїв, захист фізичних слідів на цифрових пристроях).

3. Огляд вимог клієнта (вилучення пристроїв/даних) і планування (перегляд стратегії цифрового форензіку згідно з отриманими доказами та вимогами клієнта).

4. Обробка даних у лабораторії (фізичний огляд і запис пристрою).

5. Збір даних (вибір варіантів вилучення даних).

6. Обробка даних і полегшення набору даних (перегляд вмісту пристрою).

7. Аналіз, інтерпретація та оцінювання (визначення гіпотези, інтерпретування інформації з пристроїв, попередні оціночні висновки).

8. Презентація результатів (повідомлення результатів форензіку, підготовка звіту).

9. Експертна перевірка (процес рецензування результатів перевірки).

10. Завершення справи (надання клієнту звіту та цифрових доказів).

11. Оцінювання розгорнутого робочого процесу (аналіз виконаної роботи, оцінювання продуктивності).

«Рекомендації для перших служб цифрової криміналістики» (Guidelines for Digital Forensics First Responders), розроблені Інтерполом, є більш практичними, проте в сукупності з теоретичними розробками поглиблено розкривають сутність цифрового форензіку. Автори зібрали велику кількість прикладів найкращих практик цифрового форензіку та надали пропозиції для їх виконання (Interpol, 2021). Рекомендації містять ґрунтовний аналіз роботи з багатьма цифровими пристроями – від смартфонів і планшетів до хмарних сховищ та безпілотних літальних апаратів, а також наведено детальний опис кожної процедури з метою уникнення помилок і забезпечення збереження доказів.

Останнім часом значно зріс інтерес наукової спільноти до застосування штучного інтелекту (ШІ) у сфері форензік-обліку, цифрового форензіку та управління ризиками шахрайства (Zakaria et al., 2025; Syifaurachman, 2025; Guo & Tang, 2025; Zangana et al., 2025).

Бібліометричний аналіз 261 публікації з бази Scopus (2002–липень 2025) за допомогою VOSviewer та інших інструментів (Zakaria et al., 2025) демонструє експоненціальне зростання публі-

кацій після 2017 року, особливо в галузях бізнесу, менеджменту та обліку. Ключові теми: forensic accounting, fraud detection, risk management, blockchain, big data та AI. Дослідження виділяє вісім кластерів тем (governance, fraud control, professional competency, technology-enhanced audit) і підкреслює, що ШІ стає центральним елементом «smart forensics», посилюючи точність виявлення шахрайства та управління ризиками.

Інший систематичний огляд і бібліометричний аналіз (Syifaurachman, 2025) фокусується на чотирьох етапах цифрового форензіку (identification, collection, analysis, preservation). Автор детально розглядає застосування NLP, CNN та інших ML-моделей, які значно підвищують швидкість, точність і масштабованість розслідувань. Водночас виділяються серйозні виклики: algorithmic bias, privacy concerns, lack of transparency та географічна нерівність досліджень (домінування США та Європи). Рекомендується ширше впровадження explainable AI та розширення баз даних для майбутніх досліджень.

Дослідження (Guo & Tang, 2025) демонструє трансформаційний вплив ШІ (машинне навчання, NLP, deep learning) на forensic accounting. Автори систематизують застосування ШІ для автоматизованого виявлення аномалій, аналізу великих обсягів даних, прогнозування ризиків шахрайства та підтримки судово-бухгалтерської експертизи. Підкреслюється зростання ефективності розслідувань, але й наголошуються етичні проблеми, bias алгоритмів та необхідність hybrid human-AI підходів. Ця робота підтверджує триваючий перехід від традиційного до інтелектуального форензіку.

Розглянуті моделі розроблені переважно фахівцями-практиками цифрового форензіку на основі власного досвіду, а також часто зосереджені на одній конкретній сфері, що заважає розробленню загальної моделі. Аналіз методичних засад цифрового форензіку встановлено, що існують різні підходи, які мають спільну логіку, але не утворюють єдиної системи, прийнятної для стандартизації процедур цифрового форензіку.

У результаті узагальнення існуючих підходів до здійснення цифрового форензіку запропоновано його спрощену схему (рис. 1.1).

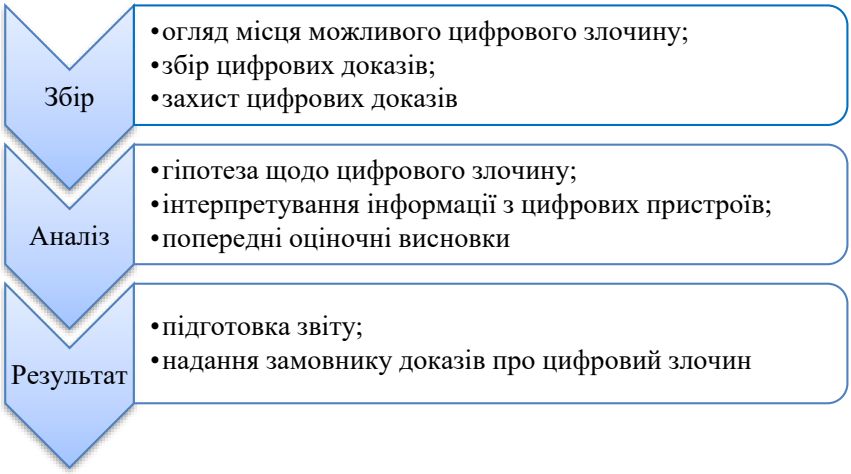

Рис. 1.1. **Спрощена схема цифрового форензіку**
Джерело: складено автором.

Цифровий форензік включає етапи збору, аналізу та надання доказів:

1. *Збір доказів.* Процес може розпочатися з перевірки систем виявлення атак, вторгнень, підозрілих записів на міжмережевому екрані (інтернет-трафіка), попереджень від системи безпеки в мережі, повідомлення окремої особи про будь-які злочини тощо. Детальне дослідження – від визначення місця комп'ютерного злочину до завершення цифрового форензіку – виконано J. Vacca (Vacca, 2005). Пошук інформації відбувається в операційних системах, електронних і зашифрованих даних. При цьому цифрові докази класифікуються. Для дослідження в рамках цифрового форензіку роблять точну копію доказу (файлу, диску) – форензік-зображення (forensic image), зміст якої має бути повністю ідентичним оригіналу (Varol & Sonmez, 2021). Дублювання даних допомагає зберігати цифрові докази. Зазвичай захист доказів виконується з метою збереження їх цілісності за допомогою криптографічних методів. Використовуються блокування запису (write blocking), відновлення даних (виявляються видалені, приховані, трансфігуровані дані), їх декомпозиція (за змістом, типом файлів та ін.), систематизація, групування, а також встановлюється значущість кожного доказу. Для захисту доказів зазначається, де саме, за яких умов і в якій ситуації їх зібрано.

2. *Аналіз доказів.* У процесі аналізу важливо отримати точні та надійні докази. Аналізуються текстові, графічні та відеофайли, вебсайти, інтернет-комунікації, миттєві повідомлення, електронна пошта; здійснюється пошук користувачів і ключових слів для пошуку додаткових даних із мережевого трафіка тощо. Для одержання уявлення про злочин і підготовки висновків про інцидент на основі наявних доказів використовуються спеціалізовані інструменти та методи критичного мислення, оцінювання, експериментування, синтезу, кореляції та перевірки (Casey, 2011). Кожна дія, рішення та метод мають бути задокументовані для забезпечення цілісності доказів за рахунок чіткого та хронологічного відстеження.

3. *Складання звіту та надання доказів.* У звіті документуються висновки, методологія та перелік доказів економічного злочину, скоєного за допомогою цифрових технологій. Звіти мають вирішальне значення для представлення доказів і забезпечення чіткого розуміння скоєного злочину та подальших дій.

Основними методами цифрового форензіку є: розшифрування та відновлення видалених файлів, зашифрованих або пошкоджених даних; вивчення даних і метаданих; дослідження мережевих комунікацій; перевірка мобільних пристроїв; перевірка жорстких дисків.

Розшифрування та відновлення видалених файлів, зашифрованих або пошкоджених даних здійснюється за допомогою інструментів цифрового форензіку, передових алгоритмів і криптографічних методів або обходу захисту паролем (наприклад, EnCase® та FTK®); включає логічне відновлення (коли програмні засоби використовуються для сканування файлової системи та відновлення видалених файлів), фізичне відновлення (ремонт пошкоджених апаратних компонентів для прямого доступу до даних), вилучення фрагментованих або частково перезаписаних файлів (аналіз базової структури файлу та пошук конкретних сигнатур файлів) (Kimmons, 2023).

Дослідження даних і метаданих необхідне для складного аналізу баз даних і комп'ютерів з метою виявлення прихованих закономірностей. Експерт вивчає інформацію про те, хто отримував доступ до бази даних та які дії було вчинено. Сучасні технології дозволяють оцінювати структуру бази даних, її вміст (бази даних реєструють взаємодію користувачів, транзакції та активність комп'ютер-

ної системи), зміни, несанкціонований доступ і видалені файли (Salvation DATA, 2023).

Аналіз мережевих комунікацій має на меті виявлення, запобігання та розслідування злочинних порушень. Мережевий трафік, у тому числі пакети даних і журнали, можна перевірити на наявність ознак вторгнення або зловмисного знищення. За наявності інтелектуальних автоматизованих інструментів кібератаки на інфраструктуру та цифрові комунікації можна виявити та звести до мінімуму (Yaacoub et al., 2022).

Перевірка мобільних пристроїв та їх операційних систем фокусується на відновленні та аналізі даних, охоплює перевірку журналів телефонних розмов, текстових повідомлень й електронних листів з метою виявлення схем спілкування, зв'язків та розмов, які можуть допомогти в розслідуванні. Використовуються спеціалізовані інструменти та методи для вилучення даних (Cellebrite, 2023).

Перевірка жорстких дисків передбачає копіювання даних секторів жорсткого диску і забезпечує надійні цифрові докази. Цей метод збору даних включає створення копії диску без зміни даних, вивчення «клону» (копії) жорсткого диска, відновлення видалених даних, визначення шкідливого програмного забезпечення (не наражаючи на ризик оригінал). Цей тип кібердоказів має бути ретельно відтворений, щоб гарантувати достовірність і надійність даних (ECS Infotech, 2024).

У результаті аналізу методологічних основ цифрового форензіку розроблено принципи, які розкривають потенціал для підвищення ефективності відповідних процедур.

1. Необхідні вимоги до форензік-експертів при отриманні цифрових доказів. Особа, яка здійснює збір даних, повинна мати компетенції для виконання цієї роботи, підтверджені сертифікацією навичок і використанням сертифікованих інструментів. Фахівець із цифрового форензіку повинен мати досвід, оскільки навіть найменша помилка під час збору даних може зруйнувати весь процес. Інструментом підтвердження фаховості форензік-експерта може виступати його сертифікація спеціально створеною самоврядною організацією, яка розробляє та затверджує відповідні стандарти здійснення форензік-діяльності, а також забезпечує моніторинг їх дотримання свої членами.

2. Умови поводження з доказами, отриманими під час цифрового форензіку. Великі обсяги цифрових доказів можуть бути

одночасно знищені або змінені. У зв'язку з цим дуже важливо зберегти цифрові докази в їхньому первинному стані на момент події.

3. Вимоги до інструментів, що використовуються для здійснення цифрового форензіку. Швидкий розвиток цифрових технологій потребує від фахівця з цифрового форензіку завжди бути обізнаним у сфері новітніх технологій, доступних на ринку, що передбачає необхідність удосконалювати свої навички для роботи з цими інструментами. Відповідно, розуміння вимог до інструментів є складовою фаховості експерта (п.1).

Таким чином, на основі аналізу сутності цифрового форензіку та діяльності експертів у цій сфері встановлено, що він має на меті не лише пошук винного в цифровому шахрайстві, а також надання вичерпних і неупереджених доказів економічного злочину. Це новий ефективний «інструмент» економічної безпеки підприємства, що допомагає попередити й уникнути цифрового корпоративного шахрайства, втрати активів та шкоди бізнесу. А поєднання традиційного економічного форензіку з цифровим надає нового імпульсу при пошуку доказів шахрайства, крадіжок, неправомірних дій співробітників, корупції тощо, оскільки цифровий слід практично не можна ліквідувати як паперові докази економічного злочину.

Додатковими напрямами діяльності експерта з форензіку для підвищення економічної безпеки підприємства є відновлення (знищення) даних, шифрування (дешифрування), пошук прихованих файлів, ідентифікація злочинців за допомогою IP-номерів, збір інформації про діяльність підприємства та його контрагентів, надання консультацій фахівцям підприємства з IT-технологій та ін.

Висновки до розділу 1

1. Стрімкий розвиток цифрових технологій обумовлює зростання кількості економічних злочинів, що потребує відповідного підвищення рівня економічної безпеки, а також активізації в розслідуванні таких злочинів, вчинених у тому числі через мережу Інтернет чи інші електронні засоби. Тому актуальним є питання поєднання традиційних, сучасних і перспективних організаційно-технологічних заходів й інструментів підвищення рівня економічної безпеки, серед яких традиційний та цифровий форензік, для виявлення

економічних злочинів, а також попередження ризиків їх виникнення на підприємствах.

2. Виявлено суттєву різницю в трактуванні економічної безпеки з позицій макроекономічного та індивідуального підходів: у рамках макроекономічного термін «економічна безпека» розглядається з точки зору держави як цілого (а не сукупності індивідів), а в рамках індивідуального – з точки зору особистості, людини. Онтологічна неоднорідність підходів обумовлює відмінності в розумінні економічних ризиків і загроз та, як наслідок, у визначенні мети політики забезпечення економічної безпеки. Тому термін «економічна безпека підприємства», що перебуває в смисловій площині між макроекономічним та індивідуальним рівнями, часто розглядається з позицій системного (стан, характерні риси системи, спроможність підприємства протидіяти загрозам і ризикам) та комплексного (комплекс заходів, що забезпечують стійке функціонування підприємства, економічну незалежність та протидію можливим загрозам і ризикам) підходів.

3. Оскільки дані є одним із найбільш важливих активів підприємства, і загроза втрати контролю за ними стає ключовою проблемою, обґрунтовано, що для захисту інформації доцільно застосовувати різноманітні методи, спрямовані на мінімізацію ризиків втрати даних, – автентифікацію та шифрування, контроль доступу користувачів, навчання співробітників, а також упровадження протоколів роботи з даними. На основі узагальнення проблем щодо забезпечення економічної безпеки підприємств встановлено, що найпоширенішим економічним злочином є корпоративне шахрайство, а дієвим способом боротьби з ним може стати цифровий економічний форензік – нова сфера міждисциплінарного наукового знання на перетині економіки та права, яка активно розвивається, має практичне застосування та перспективи подальшого розвитку.

4. Уперше у вітчизняному науковому просторі висунуто й аргументовано гіпотезу про те, що економічний форензік відповідає інституціональній парадигмі через вивчення процесів впливу на рішення економічних агентів й урахування норм і правил поведінки. На основі узагальнення результатів досліджень щодо визначення категорії «економічний форензік» встановлено, що формування загальновживаної дефініції перебуває в процесі становлення.

5. За результатами аналізу сутності економічного форензіку, його методів, а також порівняння з іншими видами економічних

«перевірок» підприємств (наприклад, внутрішнього та зовнішнього аудиту, судово-бухгалтерської експертизи) удосконалено визначення терміна «економічний форензік» як дослідження передумов та наявності економічних злочинів на підприємствах із використанням методів й інструментів економічного аналізу (економіка) та фінансових розслідувань (право) з метою одержання інформації щодо встановлення фактів та обставин економічних злочинів для прийняття управлінських рішень й удосконалення стану економічної безпеки.

6. Сформульовано об'єкт і предмет дослідження економічного форензіку: об'єкт – економічні злочини на підприємствах і поведінка економічних злочинців; предмет – закономірності дослідження об'єктів на основі спеціальних знань, трансформованих у систему методів, інструментів і засобів вирішення питань щодо виявлення економічних злочинів.

7. З урахуванням посилення ролі інформаційно-комунікаційних технологій у життєдіяльності людини розглянуто окремий напрям економічного форензіку – цифровий форензік як важливий інструмент дослідження широкого кола питань щодо опанування цифрових економічних злочинів (витоку даних, кіберзлочинності, неправомірних дій працівників, крадіжок інтелектуальної власності тощо). У рамках дослідження методології цифрового форензіку дістало подальшого розвитку структурування та визначення його процесу та завдань. Запропоновано базову схему процесу цифрового форензіку, яка, на відміну від існуючих, містить узагальнену, концентровану та вичерпну інформацію про його основні етапи. Результати аналізу низки моделей форензіку свідчать, що інші етапи, запропоновані науковцями, є другорядними, а отже, їх можна розглядати як підетапи.

8. Дістали подальшого розвитку основні принципи цифрового форензіку: необхідні вимоги до експертів при отриманні цифрових доказів; умови поводження з доказами, отриманими під час цифрового форензіку; вимоги до інструментів, що використовуються для здійснення цифрового форензіку.

РОЗДІЛ 2. СТАН ЕКОНОМІЧНОГО ФОРЕНЗІКУ В УКРАЇНІ ТА СВІТІ В УМОВАХ ЧЕТВЕРТОЇ ПРОМИСЛОВОЇ РЕВОЛЮЦІЇ

2.1 Аналіз економічної злочинності в Україні та світі

Як доведено в першому розділі, дослідження форензіку, з одного боку, є відносно новим явищем, а з іншого – має досить тривалу історію формування, яка уособлює в собі всю складність розвитку бізнесу. Так, функціонування підприємств будь-якої сфери економічної діяльності має особливості організації роботи, які залежать від обраної організаційно-правової форми, організаційної структури, характеристик й асортименту продуктів або послуг, надійності постачальників і внутрішньої корпоративної культури. В умовах недостатнього або недосконалого аналізу діяльності всі перелічені особливості функціонування підприємств можуть бути основою для вчинення економічних злочинів, пов'язаних із зловживанням, шахрайством та іншими порушеннями законодавства.

Ризики, пов'язані з економічними злочинами, є об'єктом застосування економічного форензіку. Як свідчать останні дослідження, проблема економічної злочинності у світі не втрачає актуальності. За результатами огляду, підготовленого у 2024 р. компанією PwC, у межах якого було опитано понад 2400 респондентів, до найбільших ризиків належать шахрайство під час закупівель, корупція, примусова праця, експортний контроль і санкції (PricewaterhouseCoopers, 2024). За оцінками Асоціації дипломованих фахівців із розслідування випадків шахрайства (ACFE), представленими у звіті 2024 р., які ґрунтуються на аналізі майже 2 тис. випадків, загальні збитки склали понад 3,1 млрд дол. США (Association of Certified Fraud Examiners, 2024, p. 4).

Наявні ризики виникнення економічних злочинів обумовлюють різні реакції бізнесу в світі. Наприклад, організації по-різному використовують аналітику даних для виявлення шахрайства, марнотратства чи зловживань під час закупівель (рис. 2.1). Відносна більшість компаній виконує аналіз потенційних угод (44%) та періодичний ретроспективний аналіз здійснених платежів (36%). Відносно менша кількість компаній зосереджує увагу на аналізі транзакцій або угод після їх закриття (30%) та моніторингу платежів у

режимі реального часу з можливістю блокування вихідних платежів (29%). При цьому 18% респондентів не використовують аналітику даних для виявлення шахрайства, марнотратства чи зловживань у процесі закупівель. В епоху тотальної цифровізації та аналізу звичайних і великих даних це вказує на наявність невикористаного потенціалу для вдосконалення системи протидії економічним злочинам.

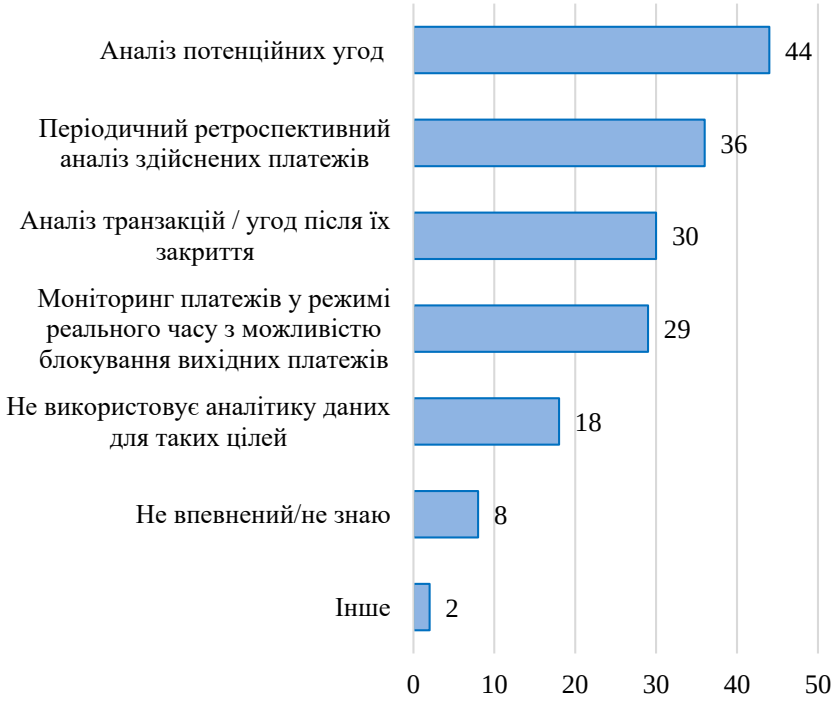

Рис. 2.1. **Відповіді на питання «Як ваша організація використовує аналітику даних для виявлення шахрайства, марнотратства чи зловживань під час закупівель?», %**
Джерело: складено за (PricewaterhouseCoopers, 2024).

Для розкриття зазначеного потенціалу доцільно проаналізувати секторальні відмінності в застосуванні аналітики даних по всьому світу (рис. 2.2). Закономірно, що компанії із сектору «технології, медіа та телекомунікації» більш активно, ніж представники

інших сфер, використовують дані для виявлення шахрайства, марнотратства чи зловживань під час закупівель (90%). Також нижче за середній рівень «нехтування аналізом даних» (18%) перебувають представники секторів «енергетика, комунальні послуги та ресурси» та «здоров'я» (15%). Натомість державні служби та сектор промислового виробництва більше за інших нехтують даними для аналізу. Так, 24 та 22% респондентів із цих секторів відповідно не використовують аналітику даних для виявлення економічних злочинів під час закупівель. Тому саме ці організації мають найбільший потенціал для підвищення рівня економічної безпеки. Слід зазначити, що досить неочікувано до цієї групи потрапили представники сектору фінансових послуг (20%), з урахуванням сучасного рівня і темпів розвитку фінансово-технологічних рішень, які переважно базуються на опрацюванні великих обсягів даних.

Рис. 2.2. **Розподіл респондентів, які не використовують аналітику даних для виявлення шахрайства, марнотратства чи зловживань під час закупівель, %**
Джерело: складено за (PricewaterhouseCoopers, 2024).

Посилюється актуальність проблематики, пов'язаної з корупцією (рис. 2.3). Так, кількість респондентів у світі, які вважають, що

ризики, пов'язані з корупцією, за останні 12 місяців зросли, вдвічі більше, ніж тих, хто вважає, що вони зменшуються (26 та 13% відповідно). Баланс відповідей між «ризики, пов'язані з корупцією, збільшуються» та «ризики, пов'язані з корупцією, зменшується» складає 13 в.п. При цьому відносна більшість респондентів дотримується позиції, згідно з якою ці ризики залишаються незмінними (43%).

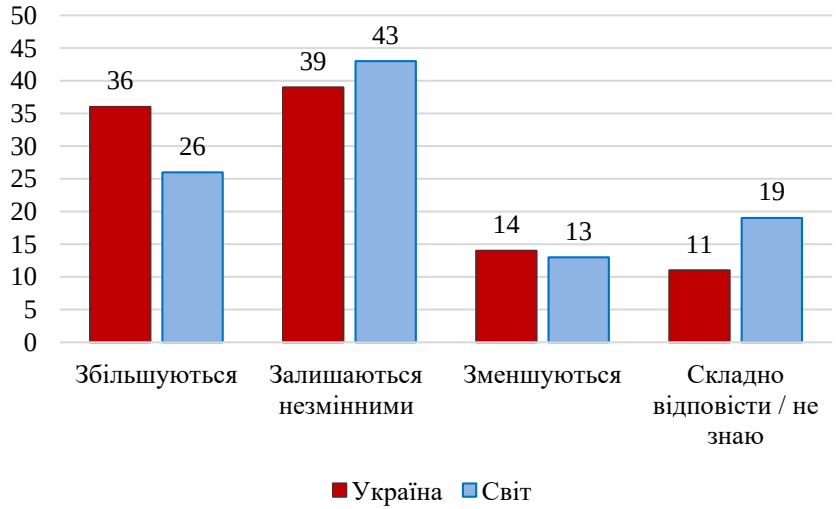

Рис. 2.3. **Відповіді на питання «На вашу думку, ризики, пов'язані з корупцією чи неправомірними виплатами державним службовцям та/або комерційним клієнтам, зросли, зменшилися чи залишилися незмінними за останні 12 місяців у країні, де ви проживаєте?», %**
Джерело: складено за (PricewaterhouseCoopers, 2024; PricewaterhouseCoopers, 2024a).

В Україні ситуація відрізняється від світової. Так, кількість вітчизняних респондентів, які вважають, що корупційні ризики за останні 12 місяців зросли, у 2,6 раза більше, ніж тих, хто вважає, що вони зменшуються (36 та 14% відповідно).

Посилення корупційних ризиків обумовлює відповідну реакцію урядів, яка навіть перевищує ступінь цих ризиків. Кількість респондентів у світі, які вважають, що зусилля урядів стають більш

наполегливими в забезпеченні антикорупційного законодавства, більше, ніж тих, хто дотримується протилежної точки зору, на 30 в.п. (рис. 2.4). Респондентів, які вважають, що діяльність урядів у цій сфері без змін, також досить багато – 41%.

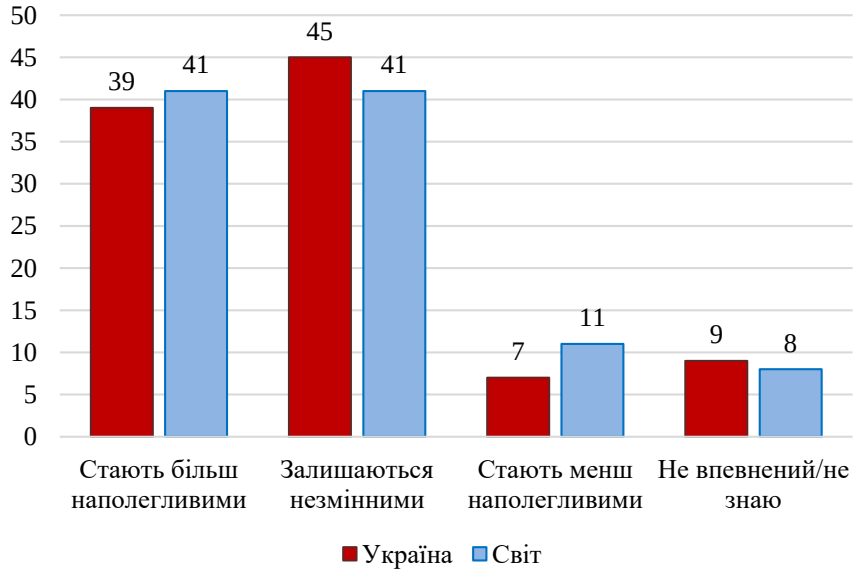

Рис. 2.4. **Відповідь на питання «Як змінюються зусилля уряду щодо забезпечення дотримання антикорупційного законодавства в країні/країнах, у яких ви працюєте?», %**
Джерело: складено за (PricewaterhouseCoopers, 2024; PricewaterhouseCoopers, 2024a).

В Україні значення даного показника дуже схожі, але тих, хто дотримується позиції, згідно з якою дії уряду щодо протидії корупційним ризикам посилюється, все ж менше, ніж у світі.

Слід зауважити, що дані результатів опитування, відображені на рис. 2.3 та 2.4, мають невелику арифметичну неточність, оскільки агреговані результати відповідей у кожному з випадків складають 101%. Імовірно, це пов’язано з накопиченням помилки через автоматичне округлення.

В епоху цифровізації провідну роль у боротьбі з корупційними ризиками відіграє аналітика даних (рис. 2.5), що охоплює

постійний моніторинг окремих типів операцій (41%), спеціальний ретроспективний аналіз операцій (35%) та агрегацію даних для забезпечення комплаєнс-моніторингу (26%). При цьому 23% респондентів у світі не використовують аналітику даних для підтримки функції комплаєнс, що свідчить про наявність невичерпаних можливостей для цього. Важливо зазначити, що в Україні даний показник нижче у понад 2 ризи та складає лише 11% (PricewaterhouseCoopers, 2024a, с. 8). Це можна пояснити тим, що прискорене поширення організації бізнес-процесів онлайн, яке потребує посиленої аналітики даних, розпочалося з глобальної пандемії COVID-19 у 2020 р. і через повномасштабну війну триває до цього часу. Натомість інші країни світу після завершення пандемії COVID-19 змогли значною мірою повернутися до стану, характерного для допандемійного періоду.

Рис. 2.5. **Розподіл відповідей на питання «Як ваша організація використовує аналітику даних для підтримки своїх цілей антикорупційної відповідності?», %**
Джерело: складено за (PricewaterhouseCoopers, 2024).

Світова практика ігнорування аналітики даних для підтримки функції комплаєнс має секторальні відмінності (рис. 2.6). Найбільш

прогресивними є представники сектору «технології, медіа та телекомунікації», де 85% підприємств використовують аналітику даних для вказаних цілей. Натомість бізнес, який представляє промислове виробництво, здійснює цю діяльність менш активно за інші сектори (29% респондентів не використовують аналітику даних), що вказує на триваючий процес імплементації концептуальних положень Індустрії 4.0 на практиці. Також відносно інших секторів низький рівень використання аналітики даних демонструють державні служби (26%).

Рис. 2.6. **Розподіл компаній за секторами, які не використовують аналітику даних для підтримки функції комплаєнс, %**
Джерело: складено за (PricewaterhouseCoopers, 2024).

Актуальність питання дотримання міжнародних прямих і вторинних санкцій посилюється для бізнесу в процесі зовнішньоекономічної діяльності в Україні та світі. Обхід санкційних режимів у певному розумінні стає окремою формою економічної злочинності в сучасному глобальному світі. Тому не випадково це питання для 44% організацій по всьому світу має вагомий пріоритет (рис. 2.7), а

ще для 24% – помірний. Відповідно низький і нульовий пріоритет це питання має лише для 30% організацій.

Рис. 2.7. **Розподіл відповідей на питання «Наскільки управління санкційними ризиками є пріоритетом у вашій організації?», %**

Джерело: складено за (PricewaterhouseCoopers, 2024; PricewaterhouseCoopers, 2024a).

В Україні спостерігається дещо інша ситуація. Для абсолютної більшості вітчизняних організацій (61%) управління санкційними ризиками є вагомим пріоритетом і лише для 25% має низький пріоритет або взагалі не є пріоритетом.

У процесі дотримання санкційних режимів у світі найбільші ризики концентруються з боку третіх сторін (63%), наприклад постачальників, і прямих клієнтів (43%). Власні бізнес-процеси та юрисдикції здійснення бізнес-діяльності містять меншу загрозу (рис. 2.8). Їх частка складає менше третини.

Рис. 2.8. **Розподіл відповідей на питання «Що з наведеного нижче, на вашу думку, становить найбільший ризик, стосовно дотримання санкцій для вашої організації?», %**
Джерело: складено за (PricewaterhouseCoopers, 2024).

Також менше третини представників бізнесу вважають, що нові технології значною мірою підвищать ефективність програми дотримання санкцій (зокрема скоротять витрати). Аналогічна кількість респондентів (31%) не передбачають, що вони матимуть суттєвий вплив на їх програму дотримання санкцій протягом наступного року (рис. 2.9).

Проблематика, пов'язана з дотриманням санкцій, тобто формуванням відповідних інститутів на рівні організації, є маркером кризи в глобалізаційних процесах, що останнім часом має тенденцію до посилення.

Найбільше поширеним видом шахрайства у світі залишається привласнення активів (рис. 2.10). Частка таких випадків становить станом на 2024 р. 89%, що на 11 в.п. більше, ніж 4 роки тому. Другим за поширенням видом шахрайства є корупція, яка мала місце у 48% випадків. Важливо зазначити, що відносна кількість випадків,

Рис. 2.9. **Розподіл відповідей на питання «Якщо говорити про нові технології та системи (наприклад, штучний інтелект, включаючи машинне навчання, або генеративний штучний інтелект), то який, на вашу думку, вплив вони матимуть на вашу програму дотримання санкцій у наступні 12 місяців?», %**
Джерело: складено за (PricewaterhouseCoopers, 2024; PricewaterhouseCoopers, 2024a).

пов'язаних із корупцією, за 2020-2024 рр. значно скоротилася – на 13 в.п. (з 61 до 48%). Найменш поширеним видом залишається шахрайство з фінансовою звітністю, частка якого складає лише 5% (станом на 2024 р.) та має суттєву тенденцію до зниження (удвічі порівняно з 2020 р.).

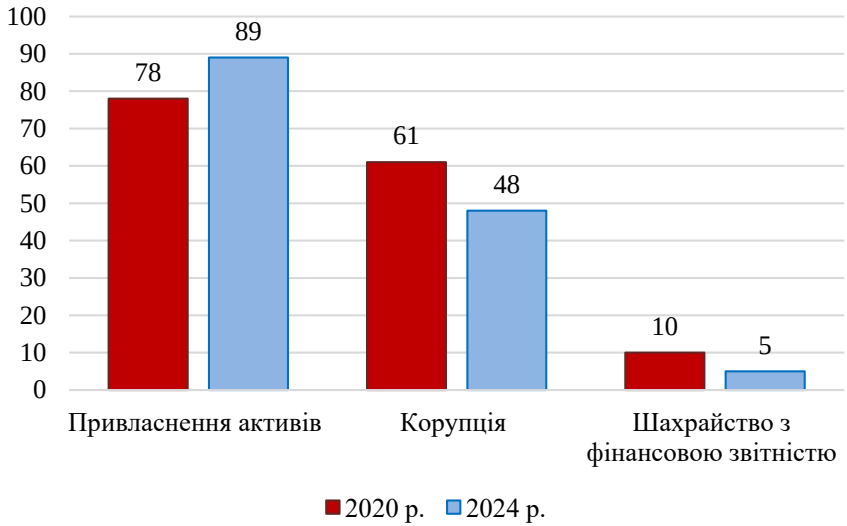

Рис. 2.10. **Розподіл видів шахрайства у 2020 та 2024 рр., %**
Джерело: складено за (Association of Certified Fraud Examiners, 2020, p. 10; Association of Certified Fraud Examiners, 2024, p. 10).

Таким чином, у першу чергу під загрозою опиняється капітал підприємства, а вже в другу – доходи, що генеруються на його основі. При цьому треба враховувати, що демаркація між відповідями є досить розмитою, оскільки корупція може бути складовою як привласнення активів і «відмивання» коштів, так і махінацій із фінансовою звітністю.

Важливим параметром є не тільки кількість, але й економічна якість, яка характеризується медіанним рівнем збитків (рис. 2.11). Як свідчать результати розрахунків, найбільші збитки в світі виникають при шахрайстві з фінансовою звітністю. Медіанні збитки за цим видом шахрайства складають 766 тис. дол. США станом на 2024 р., що у 6,4 раза більше, ніж у випадку привласнення активів, та у 3,8 раза більше, ніж при корупції. При цьому важливий аспект полягає в тому, що медіанні збитки від шахрайства з фінансовою звітністю мають тенденцію до зниження (порівняно з 2020 р.), а від привласнення активів – до збільшення. У випадку корупції медіанні збитки залишаються незмінними (200 тис. дол. США у 2020 та 2024 рр.).

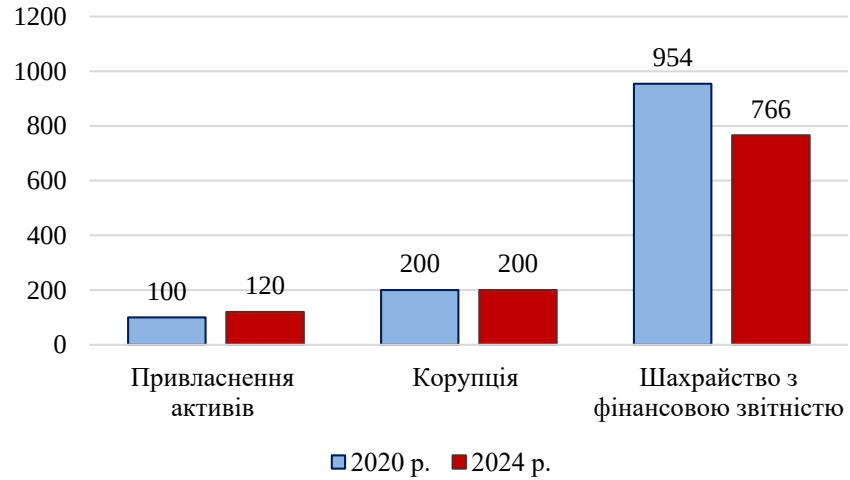

Рис. 2.11. **Медіанні збитки у 2020 та 2024 рр., тис. дол. США**
Джерело: складено за (Association of Certified Fraud Examiners, 2020, p. 10; Association of Certified Fraud Examiners, 2024, p. 10).

Заслуговує на увагу взаємозв'язок видів шахрайства (табл. 2.1). Найбільш поширеною композицією видів шахрайства є поєднання «привласнення активів» та «корупції», частка якого складає 35%. На варіанти композицій припадає разом менше 4%. Отже, корупція є важливим чинником посилення ризиків привласнення активів.

Таблиця 2.1. **Взаємозв'язок видів шахрайства (2024 р.), %**

Вид	Взаємозв'язок						
Привласнення активів	X			X	X		X
Корупція		X		X		X	X
Шахрайство з фінансовою звітністю			X		X	X	X
Кількість випадків, %	51	10	1	35	1	<1	2

Джерело: складено за (Association of Certified Fraud Examiners, 2024, p. 12).

Наступним аспектом, який потребує аналізу, є первинне джерело виявлення шахрайства (табл. 2.2). У більш ніж половини випадків виявити шахрайство вдається за допомогою «наведення», і частка таких випадків збільшується (51% у 2020 р., 56% у 2024 р.). Зі

значним відставанням друге місце посідає внутрішній аудит – його частка у 2024 р. складає 15%. Наступним джерелом виявлення шахрайства є перевірка керівництва (9%). За останні 4 роки посилив свої позиції зовнішній аудит (2% у 2020 р., 6% у 2024 р.). Частка інших першоджерел виявлення шахрайства дорівнює 3% та менше.

Таблиця 2.2. **Первинні джерела виявлення шахрайства у Східній Європі та Західній/Центральній Азії (2020 та 2024 рр.), %**

Першоджерело виявлення шахрайства	2020	2024	Зміна, в.п.
Наведення («сигнал від інсайдерів»)	51	56	5
Внутрішній аудит	14	15	1
Перевірка керівництва	9	9	0
Зовнішній аудит	2	6	4
Зізнання	1	3	2
Випадково	2	3	1
Автоматизований моніторинг транзакцій/даних (ІТ-контроль)	2	3	1
Інше	6	2	-4
Звірка рахунків	3	2	-1
Експертиза документів	3	2	-1

Джерело: складено за (Association of Certified Fraud Examiners, 2020, p.64; Association of Certified Fraud Examiners, 2024, p.84).

Результати, наведені в табл. 2.2, свідчать про те, що зовнішній і внутрішній аудит не забезпечує достатнього рівня протидії економічній злочинності. Відповідно, об’єктивно існує ніша для використання економічного форензіку.

Незважаючи на те що зовнішній аудит лише у 6% випадків є джерелом виявлення шахрайства, саме він виступає найбільш поширеною контрольною процедурою проти шахрайства, яку використовують 94% організацій (табл. 2.3). Також найчастіше разом із зовнішнім аудитом використовують кодекс поведінки (92%), внутрішній аудит (88%) та гарячу лінію (88%). Усі перелічені види контролю продемонстрували за останні 4 роки розширення застосування серед організацій (зростання від 5 до 12 в.п.).

Таблиця 2.3. **Заходи протидії шахрайству, які є найпоширенішими в Східній Європі та Західній / Центральній Азії**

Контроль проти шахрайства	2020	2024	Зміна, в.п.
Зовнішній аудит фінансової звітності	89	94	5
Кодекс поведінки	87	92	5
Відділ внутрішнього аудиту	80	88	8
Гаряча лінія	76	88	12
Перевірка діяльності керівництва	84	80	-4
Незалежний аудиторський комітет	72	79	7
Зовнішній аудит внутрішнього контролю за фінансовою звітністю	71	79	8
Сертифікація фінансової звітності керівництвом	78	76	-2
Спеціалізований відділ або команда	58	74	16
Навчання працівників протидії шахрайству	67	68	1
Політика боротьби з шахрайством	73	67	-6
Навчання з питань шахрайства	66	62	-4
Формальна оцінка ризику шахрайства	51	60	9
Проактивний моніторинг або аналіз даних	42	56	14
Раптові перевірки	45	55	10
Програми підтримки співробітників	29	42	13
Ротація	29	18	-11
Винагороди для викривачів	9	8	-1

Джерело: складено за (Association of Certified Fraud Examiners, 2020, p.65; Association of Certified Fraud Examiners, 2024, p.85).

До інструментів контролю, які мають найбільше зростання у використанні протягом 2020-2024 рр., належать діяльність спеціалізованого відділу або команди (16 в.п.) та проактивний моніторинг або аналіз даних (14 в.п.). Це підтверджує зростаючу роль аналізу даних у протидії економічним злочинам, незважаючи на варіативність рівня його застосування, що фіксується в різних дослідженнях. Зокрема, за одними оцінками, аналітичні інструменти для виявлення шахрайських дій використовують близько 82% компаній (рис. 2.1), тоді як інші джерела наводять значно нижчий показник – лише 56% (табл. 2.3).

Попри наявний контроль, як свідчать результати діяльності, спрямованої на повернення втрачених активів, відшкодування

збитків у повному обсязі є досить малоймовірним. Так, лише у 13% випадків вдалося відшкодувати збитки в повному обсязі (рис. 2.12). Натомість у 5 разів частіше (64%) не вдається отримати навіть часткового відшкодування.

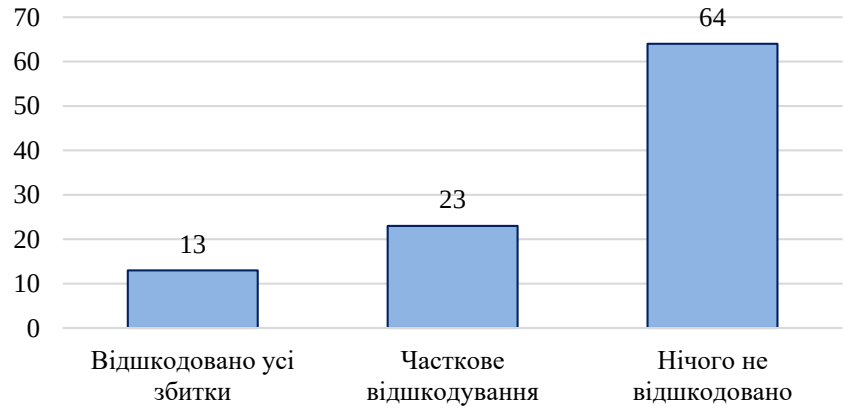

Рис. 2.12. **Ефективність організації відшкодування витрат у Східній Європі та Західній / Центральній Азії**
Джерело: складено за (Association of Certified Fraud Examiners, 2024, p.84).

Таким чином, наявні інструменти (контроль) протидії економічним злочинам мають обмежену ефективність, а отже, постає потреба в їх удосконаленні або розширенні наведеного в табл. 2.3 переліку.

З урахуванням наявної економічної злочинності можна стверджувати, що перелічені засоби запобігання випадкам шахрайства на підприємствах є обмежено надійними. Це створює необхідність пошуку альтернативних інструментів, до яких належить економічний форензік.

Для України проблема шахрайства в закупівлях є більш актуальною, ніж загалом по світу. Якщо в світі вона поширена серед 55% компаній, то в Україні – близько 70% (PricewaterhouseCoopers, 2024a).

Підтвердження гіпотези про актуальність використання економічного форензіку в Україні потребує аналізу стану економічної безпеки підприємств в Україні.

2.2 Аналіз стану економічної безпеки підприємств в Україні щодо використання цифрового форензіку

У сучасних умовах накопичення ризиків і загроз в Україні та світі загалом усе більшої актуальності набувають питання забезпечення оптимального рівня економічної безпеки підприємств, а також галузей економічної діяльності.

Невизначеність умов діяльності, вплив різних чинників внутрішнього середовища і зовнішнього оточення створюють підприємствам певні економічні ризики та порушують їх здатність нормально функціонувати, оскільки за деяких обставин реалізація економічних ризиків може трансформуватися в загрози для підприємств і таким чином створити небезпечні ситуації, які можуть призвести до економічних втрат, кризи в діяльності або навіть ліквідації підприємств.

Посилення економічних ризиків, у тому числі заснованих на цифрових технологіях (кіберзлочинність, інтернет-шахрайство, кіберкорупція, привласнення віртуальних активів, порушення інформаційної безпеки тощо), обумовлює необхідність аналізу стану економічної безпеки підприємств в Україні щодо потенціалу використання цифрового форензіку.

Сучасний етап розвитку економіки відзначається посиленням цифровізації в усіх сферах діяльності, а також наявністю загрозливо-кризових обставин (пандемії, воєнні конфлікти, глобальна зміна клімату) для нормального функціонування держави, підприємств і громадян, також характеризується поширеністю економічних злочинів. Швидке впровадження нових технологій дозволяє фінансовому шахрайству швидко оновлюватися й адаптуватися до нестабільних умов, у яких функціонують суб'єкти господарювання. Аналіз даних, відображених у наведених дослідженнях щодо наявності шахрайства й економічних злочинів в Україні, свідчить про те, що майже в половини вітчизняних підприємців виникали подібні проблеми. Це призводить до загрозливих наслідків для діяльності підприємств, що негативно впливає на економічну безпеку, репутаційні характеристики і рейтинги економічних агентів, а отже, погіршує фінансово-економічне становище загалом.

В Україні більшість підприємств не вживають жодних заходів щодо розслідування, недопущення чи попередження виникнення

фінансового шахрайства. При цьому економічні суб'єкти господарювання щорічно втрачають від 5 до 12% (Роїк, 2019) доходу через різноманітні схеми корпоративного шахрайства.

Як свідчить Всесвітнє дослідження економічних злочинів і шахрайства, проведене компанією PricewaterhouseCoopers у 2020 р., більше половини (51%) вітчизняних респондентів зазнали шкоди від шахраїв протягом останніх двох років. При цьому третина підприємств в Україні постраждала від понад двох інцидентів. Отже, якщо для всієї сукупності підприємств імовірність зіткнення з фактами шахрайства становить близько 0,5, то для компаній, які вже мали відповідний досвід, імовірність повторного зазнання економічних збитків унаслідок шахрайства оцінюється на рівні 2/3. Це означає, що проблеми в системі економічної безпеки, які вчасно не виявлені та не вирішені, неодноразово завдаватимуть збитків.

У межах вищезазначеного дослідження виокремлено п'ять найпоширеніших видів шахрайства: незаконне привласнення майна (47%), хабарництво та корупція (47%), кіберзлочини (31%), шахрайство з боку клієнтів (31%), шахрайство в закупівлях (31%). Питання щодо того, чи можна вважати окремі підгрупи видами шахрайства, залишається дискусійним, оскільки, наприклад, хабарництво та корупція не завжди відповідають загальновизнаним критеріям шахрайських дій. Разом із тим кіберзлочини є більш широкою категорією, ніж шахрайство, тому що кібершахрайство являє собою один із видів кіберзлочинів. Слід зауважити, що «незаконне привласнення майна» стосується об'єкта шахрайства (майна), «шахрайство з боку клієнтів» – суб'єктів шахрайства (клієнтів), «шахрайство в закупівлях» – діяльності підприємства або бізнес-процесу. Тому цілком закономірно стверджувати, що наведено не види, а підмножини шахрайства, які перетинаються, і це заважає одержати цілісне уявлення про стан економічних злочинів.

Незважаючи на певні методичні внутрішні протиріччя, дане опитування безумовно є джерелом унікальної та корисної інформації. Найбільш відчутних економічних втрат для відносної більшості підприємців завдано через незаконне привласнення майна (19%) та шахрайство в закупівлях (13%).

Більш вагомі загрози спостерігаються з боку зовнішнього середовища (66%), ніж внутрішнього, тобто власних співробітників (50%) (рис. 2.13). Незважаючи не це, лише половина бізнесів перевіряє доброчесність своїх контрагентів.

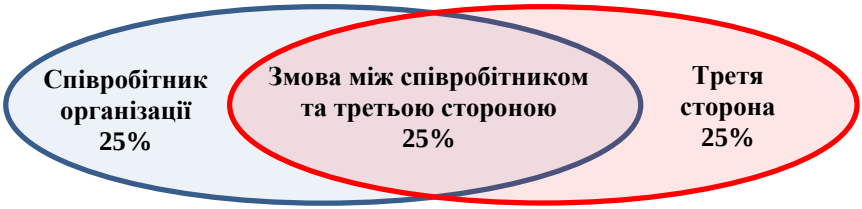

Рис. 2.13. **Внутрішні та зовнішні джерела шахрайства в Україні**
Джерело: складено за (PricewaterhouseCoopers, 2020a).

Стосовно розподілу збитків від шахрайства спостерігається важлива відмінність між Україною та світом (рис. 2.14). У світі розподіл має U-образну форму, коли кількість респондентів, які зазнали втрат в інтервалі між 100 тис. та 1 млн дол. США, менша як за кількість респондентів, які зазнали втрат нижче 100 тис. дол. США, так і за кількість тих, хто зазнав збитків понад 1 млн. дол. США. Натомість в Україні чим більшими є фінансові втрати, тим меншою є кількість респондентів, що зазнали таких збитків.

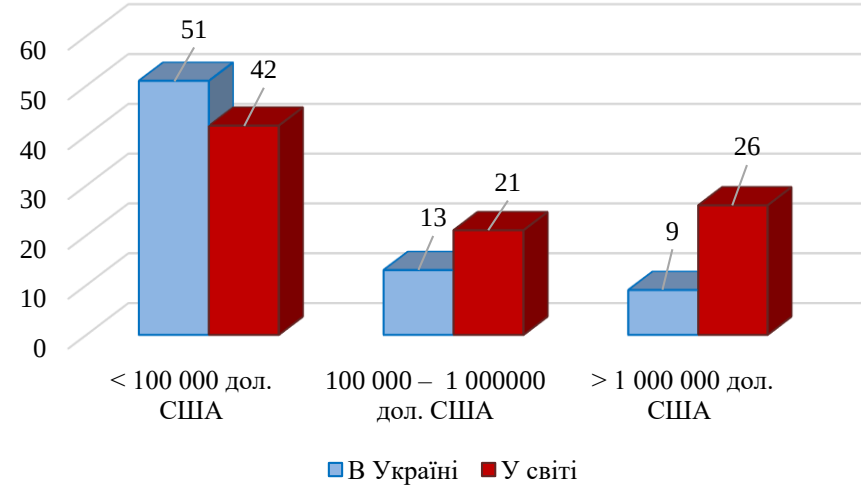

Рис. 2.14. **Розподіл збитків від шахрайства в Україні та світі (2020 р.), %**
Джерело: складено за (PricewaterhouseCoopers, 2020a).

З урахуванням триваючої євроінтеграції України можливо передбачити, що структура збитків від шахрайства змінюватиметься вбік світової. Відповідно значущість шахрайства як чинника, який має значний негативний вплив на різні сегменти бізнесу, збільшуватиметься.

При цьому варто зауважити, що наведені дані не є вичерпними, оскільки сукупний відсоток за всіма категоріями збитків не дорівнює 100% (для України – 73%, для світу – 89%). Тобто надійність цих даних має певні обмеження щодо їх статистично обґрунтованого використання.

Іншим важливим аспектом, виявленим у межах цього дослідження, є реакція на випадки шахрайства. Так «лише 59% українських організацій провели розслідування свого найгіршого випадку шахрайства» (PricewaterhouseCoopers, 2020a, с. 10). Така реакція (відмова від розслідування у 41% випадків) може пояснюватися двома чинниками: або компанія вважає, що видатки на розслідування будуть вищими за отриманий результат, або в неї немає організаційних можливостей для здійснення такого розслідування. Імовірно, саме ці дві причини обумовлюють ситуацію, за якої лише 3 із 100 компаній в Україні користуються послугами зовнішнього форензік-експерта, на відміну від показників по світу, які перевищують вітчизняні у понад 6 разів (PricewaterhouseCoopers, 2020a, с.11).

Динаміка кримінальних правопорушень проти власності в Україні вказує на наявність тренду до зменшення їх кількості (257,6 тис. у 2019 р., 113,1 тис. у 2022 р.). При цьому кількість випадків шахрайства майже не змінилася та складає дещо більше 32 тис. (рис. 2.15) Таким чином, у структурі кримінальних правопорушень проти власності частка шахрайства зросла з 12,56% у 2019 р. до 28,36% у 2022 р.

Станом на 2024 р. судовий реєстр України налічує загалом 42 787 судових вироків щодо шахрайства. За І квартал 2024 р. кількість судових рішень щодо шахрайства склала 1083. У 2023 р. кількість таких вироків вважалася найвищою і досягла 3123 (Опендатабот, 2024). Більш детально динаміку даного показника за 2020-2024 рр. наведено в табл. 2.3. За І квартал 2024 р. кількість судових вироків щодо шахрайства вже перевищує половину рішень, винесених за 2022 р., і третину вироків 2023 р. Така тенденція вказує на значне зростання кількості випадків шахрайства в поточному році.

Рис. 2.15. **Кримінальні правопорушення проти власності, включаючи випадки шахрайства, од.**
Джерело: складено за (Шикун & Булик, 2023).

Таблиця 2.4. **Динаміка кількості судових рішень щодо шахрайства в Україні за 2020-2024 рр., од.**

Показник	2020	2021	2022	2023	2024 (I квартал)
Кількість судових рішень щодо шахрайства	2 187	2 274	1 781	3 123	1 083

Джерело: складено за (Опендатабот, 2024).

За I квартал 2024 року відкрито 24 188 кримінальних проваджень за статтею 190 «Шахрайство», тобто на 20% більше порівняно з I кварталом 2023 р. Такі результати (табл. 2.5) свідчать, що в середньому у 2024 р. було відкрито щомісячно близько 8 тис. кримінальних проваджень за фактом шахрайства, що на 1 тис. справ більше, ніж у 2023 р., та в 4 рази більше, ніж у 2021 р., коли цей показник складав 2 тис. справ (Ульяненко, 2024).

Загалом в Україні у 2023 р. було відкрито більше 82 тис. кримінальних проваджень за фактом шахрайства. Ці значення були максимальними за останні 11 років. Незважаючи на таке значне

Таблиця 2.5. **Динаміка кількості кримінальних справ про шахрайство в Україні за 2021-2024 роки**

Показник	2021	2022	2023	2024 (І квартал)	2024 (5 місяців)
Кількість кримінальних справ щодо шахрайства, у тому числі:	23847	32086	82609	24188	38204
доведено до суду	8027	5778	14838	3400	7000
закрито	-	-	2150	2067	4529

Джерело: складено за (Дячкіна, 2024; Ульяненко, 2024; Опендатабот, 2024a; Опендатабот; 2024b).

зростання обсягів шахрайства, з усієї кількості зареєстрованих кримінальних проваджень тільки 18%, або 14 838 проваджень , було доведено до суду, та більше 2 тис. проваджень було взагалі закрито. У 2022 р. із відкритих кримінальних проваджень за фактом шахрайства дійшли до суду 18%, у 2021 р. – 33,6% (Дячкіна, 2024).

Аналіз сучасного стану бізнесу в Україні дозволяє припустити, що стрімке зростання шахрайства в Україні є результатом поєднання двох чинників. По-перше, це складні умови ведення бізнесу, пов'язані з воєнним станом (воєнні дії, дефіцит електроенергії та робочої сили та ін.), які посилюють невизначеність і послаблюють імунітет підприємства до протиправних дій шахрайського характеру. При цьому посилене покарання за статтею про шахрайство в умовах воєнного стану (ч. 3 ст. 190 Кримінального кодексу України) не виступає достатнім запобіжником з боку держави. По-друге, це подальше проникнення цифрових технологій, які створюють нові можливості для шахраїв.

За оцінками деяких експертів до найбільш розповсюджених видів шахрайства на підприємствах України належать (Дубцов & Борківець, 2024):

- корпоративне (внутрішнє) шахрайство;
- кібершахрайство (фішинг, фродінг, кібератаки);
- заволодіння контрагентами майном підприємств;
- рейдерство (підробка документів);
- використання назви, бренду, реквізитів підприємств (випуск продукції під іншим ім'ям, створення/дублювання сайтів).

Виокремлення таких видів є досить умовним, тому що віднесення «заволодіння майном підприємств» та «рейдерства» до видів шахрайства є неоднозначним, але наведений перелік свідчить, що корпоративне внутрішнє та кібершахрайство є найбільш розповсюдженими у практиці функціонування вітчизняних підприємств.

В умовах глобалізації бізнес-середовища, високого рівня конкуренції як на внутрішньому, так і на зовнішньому ринку та стрімкого розвитку цифрових технологій випадки корпоративного внутрішнього шахрайства можуть виникати через різноманітні причини. Так, згідно з результатами проведеного в 2023 р. опитування 400 осіб, які є керівниками підприємств, ключовими чинниками, які сприятимуть збільшенню в наступні 12 місяців кількості ризиків настання внутрішніх корпоративних злочинів, є такі (Дасюк, 2024):

кібербезпека та джерела даних (з питомою вагою 33%);
фінансовий тиск – 16%;
вплив корпоративної культури – 14%;
посилення регуляторних заходів – 13%;
геополітичне напруження – 12%.

Цей перелік чинників у вигляді рейтингу є результатом виявлених настроїв бізнесу, зокрема у процесі порівняльних заходів. Дослідження діяльності суб'єктів господарювання в цій сфері дозволило виокремити основні причини внутрішнього корпоративного шахрайства.

Розглянуті найбільш поширені види шахрайства та зростаючі значення показників щодо відкриття кримінальних справ через шахрайство останнім часом свідчать про посилення економічних ризиків, у тому числі обумовлених подальшим розгортанням цифрових технологій. У даному контексті виникає питання об'єктивного впливу цієї ситуації на фінансово-економічні результати діяльності вітчизняних підприємств.

Динаміка фінансових результатів діяльності підприємств в Україні (табл. 2.6) вказує на те, що, незважаючи на складний бізнес-клімат, кількість прибуткових підприємств стабільно перевищує кількість збиткових. І посилення шахрайства не має критичного впливу на фінансові результати економічної діяльності. При цьому вітчизняні підприємства (принаймні більша їх частина, яка є прибутковою) мають фінансові можливості для підвищення рівня економічної безпеки, у тому числі шляхом упровадження цифрового форензіку.

Таблиця 2.6. **Динаміка фінансових результатів діяльності підприємств в Україні за 2010-2024 рр.**

Рік	Фінансовий результат до оподаткування, млн грн	Підприємства, які одержали прибуток		Підприємства, які зазнали збитку	
		% до загальної кількості підприємств	фінансовий результат, млн грн	% до загальної кількості підприємств	фінансовий результат, млн грн
2010	54405,7	59,0	189640,8	41,0	135235,1
2011	118605,6	65,1	255545,9	34,9	136940,4
2012	75670,3	64,5	248036,0	35,5	172365,7
2013	11335,7	65,9	209864,5	34,1	198528,8
2014	-564376,8	66,3	233624,7	33,7	798001,5
2015	-348471,6	73,7	387652,3	26,3	736124,0
2016	69887,8	73,4	443012,1	26,6	373124,3
2017	236952,1	72,8	593168,2	27,2	356216,1
2018	369212,3	74,3	668893,5	25,7	299681,2
2019	613044,0	74,0	869642,1	26,0	256598,1
2020	134734,3	71,4	673978,8	28,6	539244,5
2021	1034012,8	73,3	1266456,3	26,7	232443,6
2022	-216594,8	66,1	724687,6	33,9	941282,4
2023	573275,1	71,0	1049205,3	29,0	475930,1
2024 (І квартал)	253585,1	73,2	319607,2	26,8	66022,1

Джерело: складено за (Державна служба статистики України, 2024).

Важливими характеристиками стану економічної безпеки підприємств є їхня забезпеченість кадровими ресурсами, обсяг реалізованої продукції та рівень рентабельності, які можна дослідити на основі аналізу даних про діяльність вітчизняних підприємств за 2010-2022 рр. (табл. 2.7).

Кількість діючих підприємств із 2019 р. стала зменшуватися та в 2022 р. мала найнижче за останні 12 років значення – 261924 од., що свідчить про наявність і суттєвий вплив загрозливих чинників зовнішнього середовища для нормального функціонування, економічної безпеки і розвитку бізнесу в Україні. Кількість зайнятих і найманих працівників зростала з 2016 до 2021 р., а в 2022 р.

зменшилася до 5,38 і 5,34 млн осіб відповідно, тобто більш ніж на 1 млн, і мала теж найнижче значення починаючи з 2012 р.

Таблиця 2.7. **Показники діяльності вітчизняних підприємств за 2010-2022 рр.**

Рік	Кількість діючих підприємств, од.	Кількість зайнятих працівників, млн осіб	Із них кількість найманих працівників, млн осіб	Обсяг реалізованої продукції (товарів, послуг), млн грн	Рівень рентабельності операційної діяльності, %	Рівень рентабельності всієї діяльності, %
2010	378810	7,96	7,84	3366228,3	4,0	0,5
2011	375695	7,79	7,71	3991239,4	5,9	1,8
2012	364935	7,68	7,58	4203169,6	5,0	1,0
2013	393327	7,41	7,29	4050215,0	3,9	-0,7
2014	341001	6,30	6,19	4170659,9	-4,1	-14,2
2015	343440	5,89	5,78	5159067,1	1,0	-7,3
2016	306369	5,80	5,71	6237535,2	7,4	0,6
2017	338256	5,81	5,71	7707935,2	8,8	3,0
2018	355877	5,96	5,87	9206049,5	8,1	4,5
2019	380597	6,41	6,24	9639730,6	10,2	7,6
2020	373822	6,37	6,29	10049870,8	6,2	0,9
2021	370834	6,39	6,29	13616793,2	12,6	10,1
2022	261924	5,38	5,34	11033018,1	3,3	-3,2

Джерело: складено за (Державна служба статистики України, 2024а).

Зменшення кількості діючих підприємств є опосередкованою ознакою зниження рівня економічної безпеки. Падіння чисельності зайнятих обумовлює посилення дефіциту персоналу необхідної кількості та якості, що формує загрози для адекватного кадрового забезпечення. Це, своєю чергою, збільшує ризики для ефективного функціонування бізнес-процесів, а отже, негативно впливає на спроможність підприємств забезпечувати релевантний рівень економічної безпеки.

В умовах воєнного стану та повномасштабних бойових дій рівень рентабельності операційної діяльності та всієї діяльності вітчизняних підприємств за 2022 р. мав неймовірно низьке значення. У 2021 р. рентабельність була найвищою починаючи з 2010 р. і складала 12,6 та 10,1% відповідно за операційною та всією діяльністю підприємств. Проте у 2022 р. вона зменшилася до 3,3% за операційною діяльністю та стала від'ємною (-3,2%) за всією діяльністю підприємств. Таке економічне становище формує діалектичне протиріччя: з одного боку, погіршення фінансових показників свідчить про незадовільний стан економічної безпеки, а з іншого – зменшення фінансових можливостей обмежує спроможність для підвищення її рівня.

Ще однією групою показників для визначення стану економічної безпеки підприємств з позиції використання цифрового форензіку є обсяг капітальних інвестицій, у тому числі інвестицій у нематеріальні активи, а саме у придбання програмного забезпечення, яке є необхідним чинником бізнес-діяльності в цифрову епоху. Динаміку обсягу капітальних інвестицій вітчизняних підприємств за 2012-2022 рр. наведено в табл. 2.8.

Аналіз даних про здійснення інвестицій підприємствами у власну діяльність свідчить, що порівняно з 2021 р. у 2022 р. загальний обсяг капітальних інвестицій зменшився на 36,8%, обсяг капітальних інвестицій у матеріальні активи – на 37, обсяг капітальних інвестицій у нематеріальні активи – на 33,4, а обсяг інвестицій у придбання програмного забезпечення – лише на 13%.

Слід зауважити, що капітальні інвестиції в придбання програмного забезпечення у 2022 р. займають в інвестиціях у нематеріальні активи 47,73%, тобто менше половини, а в загальних капітальних інвестиціях – лише 2,83%.

Зменшення обсягів капітальних інвестицій у діяльність підприємств створює ризики для зниження рівня економічної безпеки в майбутньому. Збільшення частки програмного забезпечення в структурі інвестицій свідчить про триваючу цифрову трансформацію та обумовлює гіпотезу, згідно з якою вирішення проблеми забезпечення економічної безпеки в складних зовнішніх умовах можливе з використанням цифрових інструментів. Це також стосується протидії економічним ризикам і загрозам шахрайства шляхом застосування економічного цифрового форензіку.

Таблиця 2.8. **Обсяг капітальних інвестицій підприємств України у 2012-2022 рр.**

Рік	1. Капітальні інвестиції (КІ) усього, млн грн	1.1 КІ у матеріальні активи, млн грн	1.2 КІ у нематеріальні активи, млн грн, з них	1.2.1 КІ у придбання програмного забезпечення (ПЗ), млн грн	Питома вага КІ у придбання ПЗ у капітальних інвестиціях усього, % (5/2)	Питома вага КІ у придбання ПЗ у КІ в нематеріальні активи, % (5/4)
2012	235684,8	227389,8	8295,0	2694,1	1,14	32,48
2013	222671,0	212208,1	10463,0	2687,5	1,21	25,69
2014	183954,5	176712,6	7241,9	2314,4	1,26	31,96
2015	218801,8	200590,4	18211,3	3766,4	1,72	20,68
2016	288142,6	276466,6	11676,0	4785,0	1,66	40,98
2017	366116,3	349938,4	16177,9	6443,1	1,76	39,83
2018	480314,1	444177,2	36136,9	6869,9	1,43	19,01
2019	533729,0	510940,1	22788,9	7455,3	1,40	32,71
2020	409065,4	384496,5	24568,9	8237,8	2,01	33,53
2021	545219,7	514549,6	30670,0	11207,3	2,06	36,54
2022	344303,2	323872,9	20430,3	9750,8	2,83	47,73

Джерело: складено за (Державна служба статистики України, 2024b).

Таким чином, у процесі аналізу стану економічної безпеки підприємств в Україні щодо використання цифрового форензіку встановлено, що високі значення кількості відкриття кримінальних справ через шахрайство останнім часом, особливо у 2023-2024 рр., свідчать про поширення економічних загроз для підприємств, що набуває особливого значення в умовах прискореного впровадження цифрових технологій.

Динаміка фінансових результатів діяльності підприємств в Україні вказує на недостатність їхнього потенціалу для забезпечення економічної безпеки та стабільного розвитку, а також на необхідність вживання більш ефективних заходів, серед яких цифровий форензік, щодо захисту, недопущення, мінімізації впливу загроз.

2.3 Система форензіку в контексті забезпечення економічної безпеки в Україні

Як засвідчив аналіз, викладений у підрозділі 2.2, закономірним є затребуваність послуг, пов'язаних з економічним форензіком. Попит відповідно формує пропозицію. На світовому ринку послуг щодо проведення економічного форензіку ключове місце посідає так звана «велика четвірка аудиторських компаній»: Deloitte, Ernst&Young, PwC, KPMG. Ці компанії здійснюють не лише аудит діяльності підприємств та організацій, але і консалтинг, пов'язаний із розвитком бізнесу клієнтів. Україна входить до країн, де представлені всі ці компанії, кожна з яких надає послуги, пов'язані з економічним форензіком.

Компанія Deloitte (в Україні) декларує наявність команди із 75 фахівців. Послуги в цій сфері стосуються: розслідування фінансового шахрайства (виявлення потенційно сумнівних угод, проведення внутрішніх розслідувань несумлінної поведінки керівництва та працівників); протидії хабарництву та корупції; представлення інтересів клієнтів в арбітражних інституціях; забезпечення комунікації зі страховиками та перестраховиками; перевірки благонадійності ділових контактів; управління ризиками перевищення проєктної вартості при будівництві; протидії «відмиванню» – легалізації доходів, отриманих злочинним шляхом; управління ризиками фінансового шахрайства і комплаєнс; побудови системи «гарячої лінії».

У цьому процесі використовуються такі методи та підходи: аналіз бухгалтерських записів; аналіз електронних даних; аналіз фінансової звітності; інтерв'ювання персоналу; інтерв'ювання сторонніх осіб; аналіз функціонування програми комплаєнс; діагностика заходів протидії хабарництву; аналіз контролю щодо протидії хабарництву; оцінювання збитків; дослідження репутації об'єкта, бізнес-активів, зв'язків партнера; аналіз вартості та якості робіт (при будівництві); оцінювання вірогідності виникнення ризиків шахрайських дій; аналіз великих масивів даних (Deloitte, 2025).

Компанія Ernst&Young декларує наявність 4 тис. фахівців у понад 150 офісах світу у сфері економічного форензіку, які надають такі послуги: розслідування та комплаєнс (удосконалення комплаєнс-програми); арбітражне, судове та позасудове врегулювання

претензій та спорів (у т. ч. зниження ризиків виникнення розбіжностей ще до укладення угоди); реагування на кіберзагрози та кіберінциденти (крадіжки персональних даних, зломи корпоративної електронної пошти, атаки з вимогами викупу); експертиза транзакцій; мінімізація потенційних збитків (включаючи потенційно корупційні платежі, з боку новопридбаного бізнесу); управління кризовими ситуаціями та реагування на інциденти (Ernst&Young, 2025).

Для реалізації цих та пов'язаних із ними послуг Ernst&Young застосовує такі методи, підходи і технології: форензік-аналітика; електронні пошукові технології; управління даними та їх аналіз протягом усього їх життєвого циклу; технології штучного інтелекту; дослідження прогалин, рання оцінка справи, обробки даних, аналізу документів, підготовки матеріалів, свідчень і доказових слухань для судового розгляду; опитування свідків; вивчення фізичних і цифрових доказів; антикорупційні перевірки; аналіз ризиків шахрайства.

Компанія PricewaterhouseCoopers пропонує такі послуги у сфері економічного форензіку: 1) проведення розслідування потенційного шахрайства чи зловживань; 2) розбудова організаційного потенціалу в протидії хабарництву та корупції; 3) зміцнення практики управління ризиками шахрайства; 4) підвищення ефективності протидії фінансовим злочинам; 5) зміцнення довіри та забезпечення безпеки в цифровому світі, керованому даними; 6) визначення сфери діяльності найбільш вразливої до ризиків шахрайства; 7) забезпечення сталості та безперервності бізнесу в кризових ситуаціях; 8) супровід спорів і судових процесів; 9) підвищення ефективності управління ризиками доброчесності своїх контрагентів; 10) посилення корпоративної етики та комплаєнсу; 11) здійснення більш ефективної аналітики даних; 12) підтримка в трансформації органів правосуддя (розроблення та впровадження спеціалізованих програм оптимізації); 13) тестування ефективності функціонування санкційного фільтру; 14) акселерація розвитку бізнесу; 15) розроблення цільової організаційної структури та операційної моделі для функції кібербезпеки; 16) підготовка до сертифікації за стандартами серії ISO 27000; 17) розроблення та підтримка у впровадженні політик і процедур кібербезпеки; 18) підтримка у виборі та впровадженні спеціалізованих IT-рішень; 19) підвищення рівня обізнаності з питань кібербезпеки (PricewaterhouseCoopers, 2025).

Незважаючи на те що пункт 14 не пов’язаний безпосередньо з економічним форензіком, можна припустити, що опосередковано перші 13 пунктів впливають і на акселерацію бізнесу.

Для забезпечення зазначених послуг використовується: виявлення, збір, обробка, аналіз та візуалізація широкого спектру електронної інформації; аналіз облікових систем і фінансової інформації; пошук у відкритих реєстрах та базах даних; візити на об'єкт та приватний збір даних; оцінювання та розрахунок потенційних негативних наслідків; перевірка відповідності законодавству політик і процедур; ідентифікація ризиків шахрайства та оцінювання їхньої імовірності, а також масштабу потенційного впливу; визначення «наявних внутрішніх контролів, спрямованих на протидію існуючим ризикам шахрайства та оцінювання їх дизайну й операційної ефективності»; «виявлення та оцінювання залишкових ризиків шахрайства внаслідок недостатньої ефективності існуючих або відсутності необхідних внутрішніх контролів»; «пріоритизація залишкових ризиків шахрайства на основі їх потенційної імовірності та масштабу потенційного впливу»; виявлення підозрілих транзакцій; імплементація процесів моніторингу транзакцій згідно з локальними правовими нормами; аналіз ефективності операційних моделей моніторингу транзакцій; огляд поточного стану системи управління кібербезпекою; оцінювання потенційних ризиків кібербезпеки та розроблення плану реагування на них (PricewaterhouseCoopers, 2025).

Доцільно розглянути запропоновану фахівцями PwC модель проведення форензік-діагностики (рис. 2.16), яка складається з трьох етапів. Слід зауважити, що назва (форензік-діагностика) лише частково відповідає змісту. Якщо перший етап «аналіз поточного стану» певною мірою можна вважати складовою діагностики, то розроблення рекомендацій та реалізацію необхідних змін складно віднести до діагностики.

Так, другий етап «розроблення рекомендацій та підготовка до їх упровадження» є не стільки діагностикою, скільки результатом використання інформації, отриманої в межах здійсненої діагностики. Ще більш нерелевантним вбачається включення до діагностики етапу «реалізація необхідних змін».

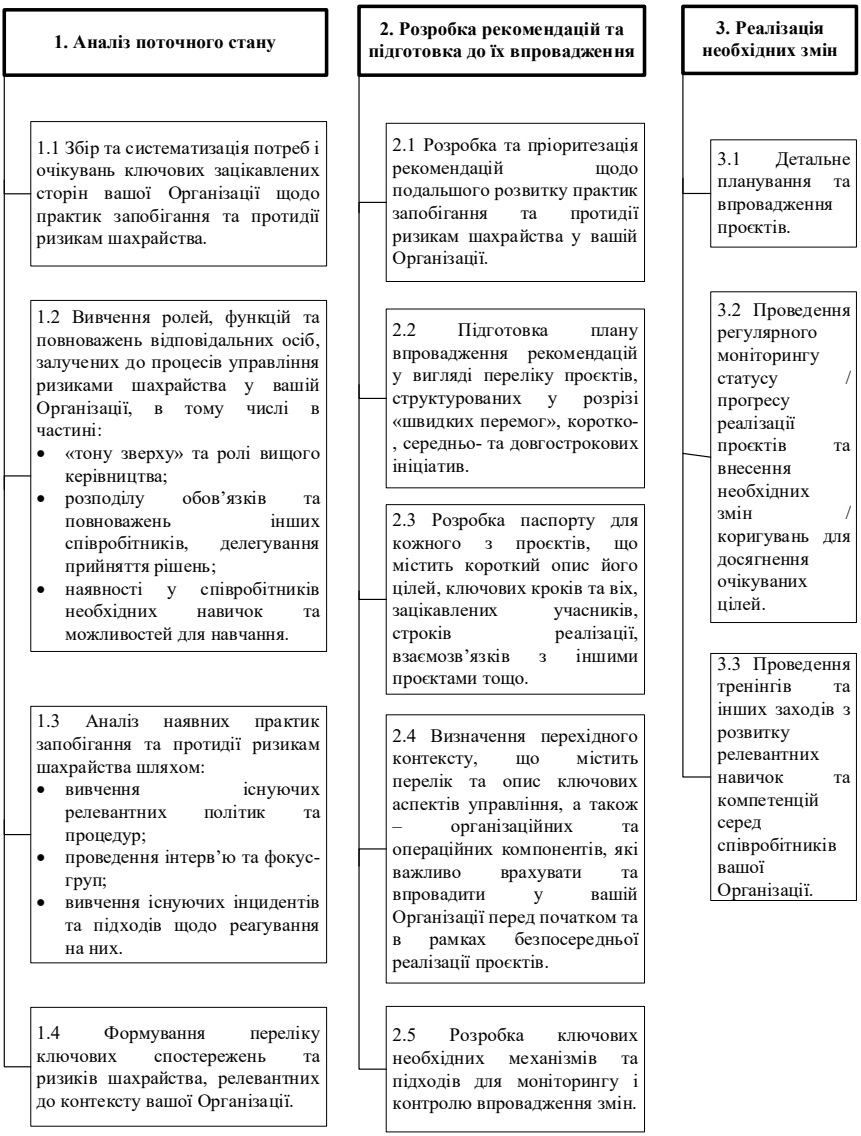

Рис. 2.16. **Форензік-діагностика з позицій компанії PricewaterhouseCoopers**

Джерело: складено за (PricewaterhouseCoopers, 2024b).

Фактично цією компанією запропонований підхід, у рамках якого реалізується логіка «as is» – «to be» – «to do» («як є»-«як має бути»-«що робити»). Тобто з початку описується ситуація, якою вона є. Потім обґрунтовується цільовий стан. І на останньому етапі визначається, які зміни необхідно здійснити, щоб досягти цільового стану.

У цьому контексті важливо зазначити, що 4 з 5 підетапів другого етапу та весь третій етап не містять згадування шахрайства. Тобто вони не містять специфіки, притаманної виключно шахрайству. Також слід зауважити, що форензік-діагностика від PwC сконцентрована виключно на шахрайстві, залишаючи поза увагою інші економічні злочини (наприклад, корупцію).

Об'єктом, на який спрямоване застосування цієї форензік-діагностики, є процес запобігання шахрайству та реагування на нього, а не його окремі випадки.

Також до «Великої аудиторської четвірки» входить KPMG. Ця компанія до послуг, пов'язаних з економічним форензіком, відносить: послуги у сфері протидії корупції; сприяння в судових спорах; розслідування шахрайства; управління ризиками шахрайства; форензік-IT.

Для забезпечення цих послуг виконується наступна робота: збереження, відновлення та аналіз електронних даних; оцінювання корупційних ризиків; інтерв'ю зі співробітниками; оцінювання заходів щодо боротьби з корупцією з позицій дизайну (як зазначено в політиках) і операційна ефективність (як працює в реальності); удосконалення чинних і впровадження нових контролів; навчання співробітників; визначення та оцінювання ризиків шахрайства; формування карти ризиків; узгодження ризиків і контролів; оптимізація існуючих механізмів контролю; визначення суми збитків; складання переліку співробітників, які могли брати участь у порушеннях; удосконалення системи внутрішнього контролю (KPMG, 2024; KPMG, 2024a).

Узагальнений перелік основних форензік-послуг, які надаються цими компаніями, в тому числі в Україні, наведено в табл. 2.9.

Звичайно, інструменти можна вважати окремими послугами або їх складовими. Наведений перелік послуг пов'язаний з економі-

Таблиця 2.9. **Послуги щодо економічного форензіку, що надаються аудиторськими компаніями «Великої аудиторської четвірки»**

Компанія	Послуги
1. Deloitte	- виявлення та зменшення ризиків виникнення шахрайства, незаконних дій і неетичної поведінки; - експрес-діагностика ризиків шахрайства; - оцінювання фінансових втрат, що виникають унаслідок незаконного привласнення та розтрати активів, а також невигідних для компанії закупівель і продажів; - упровадження найкращих практик управління ризиками, які відповідають цілям і завданням кожної компанії
2. E&Y	- реагування на передбачувані випадки хабарництва, недобросовісних та інших протиправних дій; - використання передових технологій для оперативного збору фактів і доказів, щоб оцінити масштаб проблеми; - аналіз зв'язків, схем і аномалій, а також представлення зібраних доказів під час судових розглядів; - оцінювання моделі поведінки співробітників, яку можна закласти в основу гнучких комплаєнс-програм, із застосуванням засобів форензік-аналізу
3. PwC	- проведення розслідування потенційного шахрайства чи зловживань; - супровід спорів і судових процесів; - розбудова організаційного потенціалу в протидії хабарництву та корупції; - підвищення ефективності управління ризиками доброчесності своїх контрагентів; - зміцнення практики управління ризиками шахрайства; - підвищення ефективності протидії фінансовим злочинам; - зміцнення довіри та забезпечення безпеки в цифровому світі, керованому даними; - визначення сфери діяльності найбільш вразливої до ризиків шахрайства
4. KPMG	- упровадження програми боротьби з шахрайством і корупцією; - розслідування випадків шахрайства та інших порушень; - форензік-ІТ, який передбачає збереження електронних даних для подальшого вивчення, а також відновлення видалених документів, які можуть містити докази порушень

Джерело: побудовано за (Deloitte, 2025; PricewaterhouseCoopers, 2025.; Ernst& Young, 2025; KPMG, 2024).

чним форензіком безпосередньо та опосередковано. Виконаний аналіз мав на меті не виявлення «кращої» серед компаній «Великої аудиторської четвірки», а лише окреслення практичної сфери застосування економічного форензіку.

Перелік послуг кожної з цих компаній містить економічний форензік, який або спрямований на цифрову сферу, або передбачає використання цифрових технологій у традиційній сфері (форензік-IT, eDiscovery). Цифровізація процедури економічного форензіку, з одного боку, є реакцією на поширення економічної злочинності в цифровій сфері, а з іншого – інструментом підвищення ефективності форензіку в традиційному застосуванні.

Як альтернативні варіанти перевірок на підприємствах розглядаються внутрішні перевірки (контроль), проведення зовнішнього аудиту, здійснення економічного форензіку (форензік-аудиту, форензік-розслідування). Більш детальну характеристику складових внутрішнього контролю, зовнішнього аудиту та форензіку, яку висвітлено в роботі (Семенець, 2019, с. 284), наведено на рис. 2.17. Запропонований цим дослідником порівняльний аналіз зовнішнього аудиту, внутрішнього контролю та форензік-аудиту потребує критичного аналізу з позицій відповідності існуючим фактам.

Так, визначення *регламентації* зовнішнього та форензік-аудиту потребує уточнення. Зовнішній аудит може відбуватися на замовлення клієнта і, відповідно, регулюватися нормативами не лише згідно з вимогами Міжнародних стандартів фінансової звітності, а також ураховувати внутрішні положення та вимоги клієнта. Наприклад, сам процес внутрішнього контролю та форензік-аудиту може бути об’єктом для зовнішнього аудиту, і при проведенні цього зовнішнього аудиту аудитор керуватиметься в тому числі внутрішніми положеннями та регламентами. Форензік-аудит, окрім норм чинного законодавства, також може враховувати внутрішні нормативні документи клієнта.

Щодо запропонованої *періодичності* проведення зовнішніх аудиторських перевірок у кінці звітного періоду, то слід зазначити, що вона не є обов’язково саме такою. Зовнішній аудит може здійснюватися на замовлення та за рахунок організації-клієнта в будь-який час.

Критерії порівняння	Зовнішній аудит	Внутрішній контроль	Форензік аудит
Нормативна регламентація	Міжнародні стандарти аудиту, закони, які регулюють ведення бухгалтерського обліку та аудиту, методичні рекомендації тощо	Внутрішні регламенти	Кримінальний, податковий, трудовий кодекси, кодекс про адміністративні правопорушення
Періодичність	Наприкінці звітного періоду	Регулярно	За необхідності, при виявленні фактів порушень
Мета	Підтвердження достовірності фінансової звітності	Вивчення фактичного стану активів підприємства	Виявлення та попередження махінацій та шахрайств
Суб'єкти проведення	Аудиторські фірми, зовнішні аудитори	Управлінський персонал	Внутрішні аудитори, форензік-спеціалісти
Об'єкт перевірки	Фінансова звітність	Майно підприємства	Усі внутрішні процеси, діяльність, фінансові результати
Результати перевірки	Аудиторський висновок	Внутрішні звіти	Докази здійснення чи нездійснення шахрайств
Відносини із суб'єктом господарювання	Вертикальні	Вертикально-горизонтальні	Залежить від суб'єкта здійснення

Рис. 2.17. **Порівняння зовнішнього аудиту, внутрішнього контролю та форензік-аудиту**
Джерело: побудовано за (Семенець, 2019, с. 284).

Відповідно визначена *мета зовнішнього аудиту* – підтвердження достовірності фінансової звітності – є лише окремим випадком (хоча найбільш розповсюдженим) більш широкої мети, яку встановлює замовник аудиту. *Мета внутрішнього контролю* (вивчення фактичного стану активів підприємства) є обмеженою і, наприклад, не розповсюджується на пасиви компанії. Мета форензік-аудиту – виявлення та попередження махінацій і випадків шахрай-

ства, – як і в двох попередніх випадках, не відповідає критерію повноти та є лише окремим випадком для всієї сукупності економічних злочинів.

Суб'єктом проведення внутрішнього контролю зазначено управлінський персонал, але з позицій класичного корпоративного управління ця функція (нагляд за системою внутрішнього контролю та управління ризиками) реалізується в інтересах акціонерів аудиторськими комітетами при наглядових радах (радах директорів).

Прикладом реалізації такого підходу є структура корпоративного управління Групи ДТЕК (ДТЕК, 2025). Якщо внутрішній контроль реалізується в інтересах найманого менеджменту, а не акціонерів, тоді функціонує відповідний структурний підрозділ (наприклад, департамент внутрішнього контролю). У будь-якому разі менеджмент не є безпосереднім суб'єктом здійснення корпоративного внутрішнього контролю. Він може виступати лише споживачем результатів діяльності внутрішнього контролю. При визначенні *суб'єкта проведення форензік-аудиту* також запропонована теза, яка має підстави до критичного осмислення. Науковець стверджує, що суб'єктом здійснення є лише внутрішні аудитори та форензік-фахівці без залучення аудиторських фірм, як це було зазначено у випадку зовнішнього аудиту. Однак це суперечить вищенаведеним фактам. Так, усі аудиторські компанії, які входять до «Великої аудиторської четвірки», надають такі послуги, а отже, в процесі їх надання виступають суб'єктами.

Також викликає питання *об'єкт перевірки*. Для внутрішнього контролю недоцільно обмежуватися майном підприємства, як і для аудиторської перевірки – виключно фінансовою звітністю. За умови розгляду саме такого об'єкта перевірки зовнішній аудит взагалі звужується до зовнішнього аудиту фінансової звітності, тобто залишаються поза увагою інші види аудиту (наприклад, операційний аудит, аудит системи контролю тощо). Тому доцільно як об'єкт розглядати всі бізнес-процеси (наприклад, закупівлі, систему підготовки фінансової звітності та ін.).

Результатом форензік-аудиту можуть бути не лише докази вчинення чи відсутності шахрайства, але і виявлення фактів шахрайства, оцінка збитків, ідентифікація причетних осіб, рекомендації

щодо усунення проблем, покращення системи внутрішнього контролю та запобігання аналогічним ситуаціям у майбутньому, оцінка відповідних ризиків. Тобто результат не відповідає критерію повноти.

Запропонований розподіл відносин із суб'єктом господарювання на вертикальні та вертикально-горизонтальні для зовнішнього аудиту та внутрішнього контролю видається дещо суперечливим. Так, зазначається, що суб'єкт господарювання та зовнішній аудитор перебувають у вертикальних відносинах. По-перше, не зрозуміло хто вище, а хто нижче за цією вертикаллю. По-друге, аудиторська компанія та суб'єкт господарювання укладають угоду на проведення аудиту. Відповідно, вони є двома сторонами договору однакового рівня, що вказує на горизонтальний зв'язок, а не на вертикальний.

Таким чином, запропонована А. Семенець характеристика складових внутрішнього контролю, зовнішнього аудиту та економічного форензіку має потенціал до вдосконалення.

Інший порівняльний аналіз форензіку, аудиту, інспектування та економічної експертизи виконано О. Рябчук та С. Твердуном (рис. 2.18), у рамках якого розглянуто економічний форензік, аудит, інспектування та економічну експертизу за 7 ознаками (мета, суб'єкти, нормативно-правове регулювання, характер діяльності, періодичність проведення, фінансування, користувачі інформації).

Формулювання мети для форензіку, аудиту, інспектування та економічної експертизи в цілому не викликає заперечень, але аудит обмежується виключно фінансовою звітністю, що є некоректним (як доведено вище).

Наведений у дослідженні (Рябчук & Твердун, 2021, с. 79) порівняльний аналіз ознак «суб'єкти» та «нормативно-правове регулювання», який значною мірою визначає цих суб'єктів, свідчить, що порівняно з аудитом та інспектуванням найменш конкретною та нечітко регламентованою на законодавчому рівні є процедура економічного форензіку.

Найбільші сумніви викликає ознака «користувачі інформації». Запропоновані варіанти користувачів інформації, з одного боку, є неповними, а з іншого – надмірно широкими. Так, для форензіку вказані «особи, які звернулися за послугою». Однак одержані

Ознаки	Форензік	Аудит	Інспектування	Економічна експертиза
Мета	Виявлення загроз шахрайства та (або) встановлення винної особи і збору доказів за фактом порушення	Надання об'єктивної, незалежної інформації щодо стану фінансової звітності	Виявлення фактів порушення законодавства, встановлення винних у їх допущенні посадових і матеріально відповідальних осіб	Визначається органом, що призначив проведення експертизи
Суб'єкти	Аудитори, оцінювачі, юристи, експерти	Аудитори	Державна аудиторська служба, її міжрегіональні територіальні органи	Експерти
Нормативно-правове регулювання	Орієнтується на закони та стандарти відповідних сфер	МСА, Закон України «Про аудит фінансової звітності та аудиторську діяльність»	Порядок проведення інспектування Державною аудиторською службою, її міжрегіональними територіальними органами, Закон України «Про основні засади здійснення державного фінансового контролю в Україні»	Інструкція «Про призначення та проведення судових експертиз та експертних досліджень», Закон України «Про судову експертизу»
Характер діяльності	Підприємницький (на основі договору про надання послуг)	Підприємницький (на основі договору про надання послуг)	Виконавчий (на основі плану-графіка, за наявності підстав або за рішенням суду)	Виконавчий (процесуальний документ про призначення експертизи, складений Уповноваженою на те особою (органом))
Періодичність проведення	За потреби	Раз на рік або за потреби	Не частіше разу на рік	За потреби
Фінансування	Замовник	Замовник	Державний бюджет України	Державний бюджет України
Користувачі інформації	Особи, які звернулися за послугою	Зовнішні та внутрішні	Зовнішні та внутрішні	Зацікавлені користувачі

Рис. 2.18. **Характеристика складових форензіку, аудиту, інспектування, економічної експертизи**
Джерело: (Рябчук & Твердун, 2021, с. 79).

результати можуть бути використані в судових процесах, тому судові органи також виступатимуть користувачами інформації.

Натомість для аудиту та інспектування зазначено, що існують зовнішні та внутрішні користувачі інформації. Але будь-який користувач є або зовнішнім, або внутрішнім. Відповідно, така демаркація користувачів інформації не створює доданої вартості для аналізу. Аналогічно і із «зацікавленими користувачами для економічної експертизи»: залишається невизначеним, хто саме належить до зацікавлених користувачів.

Як видно з порівняння ознак, найближчим до економічного форензіку є аудит, а інспектування та економічна експертиза мають суттєві відмінності з позицій замовника та джерел фінансування (Державний бюджет України). Якби в цій порівняльній класифікації аудит розширити за межі фінансової звітності та доповнити його внутрішнім аудитом, то в такому випадку принципова різниця між економічним форензіком та аудитом буде малопомітною. Це вказує на недостатність запропонованого переліку ознак для порівняння. Наприклад, доцільно було б доповнити його об'єктом і результатом оцінювання.

Основними відмінностями форензіку від внутрішнього контролю, аудиту та інших видів перевірок, на думку С. Тютченко, можна вважати:

- динамічність алгоритму здійснення процедури економічного форензіку;
- спрямованість на забезпечення економічної безпеки підприємства, тобто на внутрішній захист бізнесу;
- перевірку інформації з різних джерел, у тому числі неофіційних;
- побудову сценаріїв потенційних ризиків і шахрайства;
- формування превентивних заходів щодо попередження загроз;
- ініціативу проведення, форму результатів перевірки після проведення форензіку (Тютченко, 2021).

Запропоновані в роботі (Рябчук & Твердун, 2021) основні напрями форензіку (рис. 2.19) підлягають ґрунтовному осмисленню та критичному аналізу.

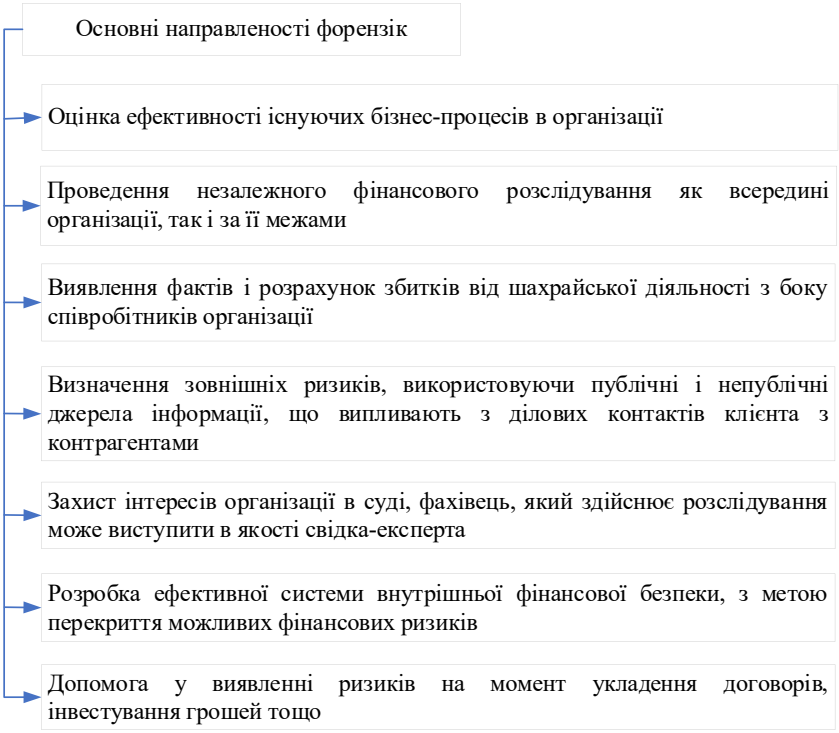

Рис. 2.19. **Основні направленості форензіку**
Джерело: складено за (Рябчук & Твердун, 2021, с. 81).

З урахуванням відсутності критерію демаркації між цими напрямами формуються ризики їх перетину. Так, як різні напрями виокремлено «проведення незалежного фінансового розслідування як всередині організації, так і за її межами» та «виявлення фактів і розрахунок збитків від шахрайської діяльності з боку співробітників організації». Проведення розслідування без виявлення фактів неможливе. Тобто другий напрям можна розглядати як складову першого. При цьому слід звернути увагу, що не можна обмежуватися лише шахрайством, ігноруючи інші економічні злочини (наприклад, корупцію), та фокусуватися виключно на «співробітниках організації», ігноруючи зовнішніх акторів.

При описі напряму «визначення зовнішніх ризиків із використанням публічних і непублічних джерел інформації, що виплива-

ють із ділових контактів клієнта з контрагентами» додано зайвий елемент «із використанням публічних і непублічних джерел інформації», оскільки «публічні та непублічні» формують повну групу, а отже, це уточнення не надає додаткової інформації. До того ж, більш відповідним логіці форензік-розслідування є виявлення не тільки ризиків, але й фактів.

Таким чином, окремі напрями потребують уточнення.

Так, до основних напрямів форензіку віднесено «оцінювання ефективності існуючих бізнес-процесів в організації», але не зазначено, з яких саме позицій передбачається таке оцінювання. До критеріїв оцінювання ефективності можна віднести: мінімізацію кількості випадків економічних злочинів (включаючи шахрайство), зменшення середнього або максимального обсягу збитків, середнього строку виявлення економічного злочину, середнього строку проведення форензік-розслідування. Без застосування цих критеріїв складається враження, що форензік спрямований на всі бізнес-процеси у всіх аспектах.

Напрям «захист інтересів організації в суді …» відповідає профілю адвокатської діяльності. Більш коректно було б акцентувати увагу на «участі в захисті інтересів організації в суді…».

Напрям «розроблення ефективної системи внутрішньої фінансової безпеки з метою перекриття можливих фінансових ризиків» є занадто «широким». Зазвичай до «фінансових ризиків» входять кредитний, процентний, валютний, ліквідності та ін., що виходить за масштаб сфери економічного форензіку.

Отже, розглянуті напрями економічного форензіку мають потенціал до вдосконалення та можуть використовуватися лише з урахуванням наведених зауважень.

Інший підхід до формування напрямів проведення економічного форензіку міститься в роботі (Чут, 2020, с. 148), де на основі виокремлених ризиків виявлено найбільш поширені напрями:

дослідження слідів шахрайства в галузі фінансів, бухгалтерського обліку, первинної документації;

цифровий (IT) форензік;

корпоративний форензік;

попередження подальшого шахрайства.

Детальну характеристику цих напрямів наведено на рис. 2.20.

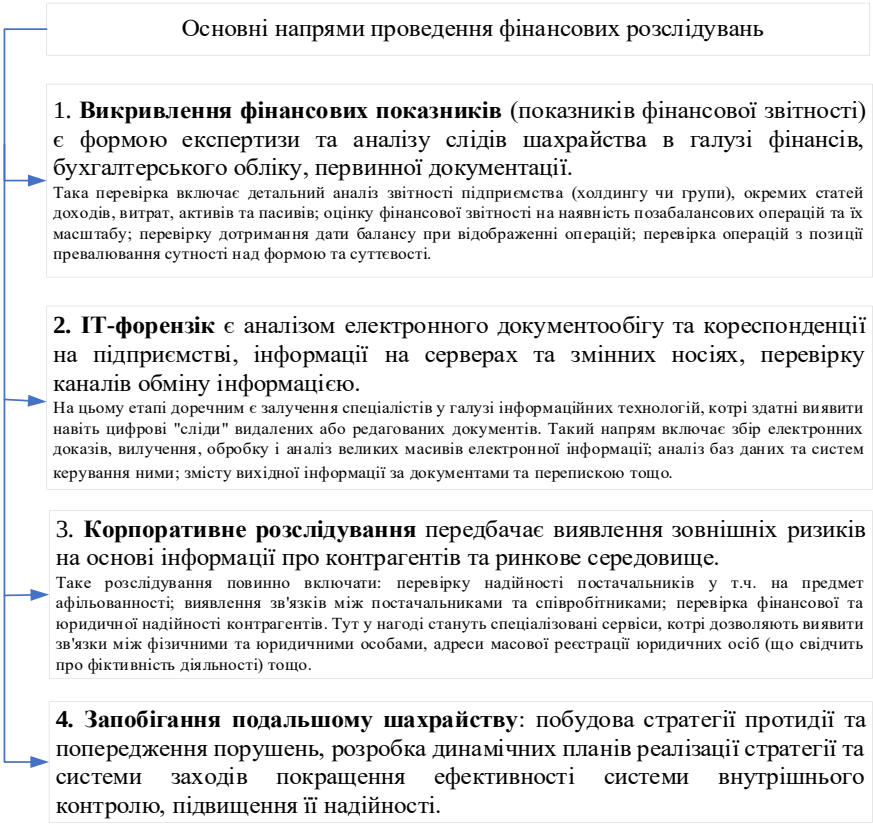

Рис. 2.20. **Основні напрями проведення фінансових розслідувань**
Джерело: складено за (Чут, 2020, с. 148).

Наведена класифікація, з одного боку, значною мірою відрізняється від попередньої, а з іншого – також містить низку недоліків. Так, перший напрям розглядається як «форма аналізу». Другий відрізняється об’єктом аналізу. У сучасних умовах, коли весь бухгалтерський облік здійснюється в цифровій формі, відокремити перший напрям від другого неможливо. Також варто зазначити, що другий напрям автор називає етапом.

Третій напрям («корпоративне розслідування») сконцентрований виключно на внутрішніх ризиках, що не узгоджується з назвою, а також перетинається з першим і другим напрямами.

Четвертий напрям («запобігання подальшому шахрайству») доцільно розглядати поза процесом форензік-розслідування, тобто він є бажаним результатом, наслідком розслідування, а не його напрямом.

Загалом дослідження складових елементів форензіку, визначення їх характеристик у порівнянні з іншими видами контролю і перевірок дозволило систематизувати отримані дані та сформувати структуру системи економічного форензіку з позиції забезпечення економічної безпеки підприємств в Україні (рис. 2.21).

Так, метою економічного форензіку є виявлення, розслідування і попередження економічних злочинів, включаючи встановлення причетних осіб.

Етапи проведення форензіку:

1. Ініціація форензіку. Ініціація форензік-розслідування уповноваженою особою. Підписання угоди в разі залучення зовнішнього суб'єкта розслідування.

2. Збір даних. Огляд місця можливого цифрового економічного злочину. Збір цифрових та аналогових доказів. Документування, захист і збереження цифрових й аналогових доказів.

3. Аналіз даних. Визначення переліку гіпотез щодо шляхів і виконавців цифрового економічного злочину. Інтерпретування та аналіз цифрової та аналогової інформації в її сукупності.

4. Оформлення результату. Підготовка звіту або висновку за результатами форензік-розслідування.

5. Подальше використання економічного форензіку. Надання рекомендацій щодо вдосконалення системи внутрішнього контролю та економічної безпеки, управління ризиками, пов'язаними з економічними злочинами та запобіганням їх негативному впливу.

Результатами економічного форензіку за сутністю є надання доказів здійснення чи відсутності економічних злочинів; рекомендації щодо вдосконалення системи внутрішнього контролю та економічної безпеки, управління ризиками, пов'язаними з економічними злочинами та запобіганням їх негативному впливу.

Результатом форензіку за формою є висновок; експертне судження для представлення в суді; резюме виявлених доказів та їх обґрунтування; розрахунок прямої та, по можливості, опосередкованої шкоди та його документальне обґрунтування.

Рис. 2.21. **Структура системи форензіку з позиції забезпечення економічної безпеки підприємств**
Джерело: складено за (Семенець, 2019, с. 284; Рябчук & Твердун, 2021, с. 79; Чут, 2020, с. 149).

Таким чином, на основі дослідження та порівняння основних структурних елементів економічного форензіку, внутрішнього контролю, зовнішнього аудиту, інспектування, економічної експертизи з позицій посилення економічної безпеки вітчизняних підприємств встановлено, що найбільш доцільним для забезпечення економічної безпеки підприємств України є використання процедури економічного форензіку. Наведено його функціональні напрями здійснення, підпроцеси цієї процедури, етапи формування системи внутрішнього контролю та економічної безпеки на підприємстві за результатами форензіку. Сформовано структуру системи економічного форензіку з позиції забезпечення економічної безпеки підприємств.

Систематичне проведення форензіку сприятиме зміцненню економічної безпеки підприємств, дозволить своєчасно ідентифікувати причинно-наслідкові зв'язки між випадками шахрайства та обставинами, що їх спричинили, а також виявляти та запобігати ризикам, пов'язаним із шахрайськими діями, незаконними вчинками та неетичною поведінкою як працівників, так і контрагентів. Крім того, цей процес уможливить підтвердження фактів порушень, оцінювання фінансових втрат, що виникають унаслідок незаконного привласнення та розтрат активів, здійснення невигідних для підприємства бізнес-процесів у сфері забезпечення, виробництва, реалізації та співпраці з партнерами.

Висновки до розділу 2

1. У результаті аналізу економічної злочинності в світі та Україні встановлено, що, незважаючи на тотальне проникнення цифрових технологій, не всі компанії використовують аналітику даних. Це свідчить про невикористані можливості цифрового економічного форензіку як інструменту протидії економічній злочинності, оскільки найбільші втрати підприємствам продовжують завдавати шахрайство під час закупівель, корупція, привласнення активів, експортний контроль і санкції.

2. Виконано оцінювання потенціалу використання цифрового форензіку для посилення економічної безпеки підприємств шляхом аналізу виявлення економічного шахрайства та застосування аналітики даних у різних секторах економіки. Встановлено,

що більшість випадків економічних злочинів вдається розкрити за допомогою «сигналів» від інсайдерів, меншою мірою – за результатами внутрішнього аудиту і перевірок керівництва. Ці дані свідчать про обмежену ефективність внутрішнього контролю на підприємствах, підвищують інтерес і створюють нішу для використання економічного форензіку з метою усунення ризиків і своєчасного виявлення ознак економічних злочинів. Визначено суттєві відмінності між секторами економіки щодо залученості й активності використання аналітики даних. З урахуванням низького рівня використання аналітики даних у секторах «державні служби», «промислове виробництво» та «фінансові послуги» запропоновано його підвищення шляхом упровадження цифрового форензіку в діяльність підприємств.

3. За результатами аналізу стану економічної безпеки вітчизняних підприємств встановлено, що найбільш поширеними видами економічного шахрайства в Україні є незаконне привласнення майна, хабарництво та корупція, кіберзлочини, шахрайство з боку клієнтів і шахрайство в закупівлях. Незважаючи на те що більш вагомі загрози спостерігаються з боку зовнішнього середовища, лише половина підприємців перевіряє доброчесність своїх контрагентів. Визначено, шо попри зростання кількості випадків економічного шахрайства та значні втрати, які воно спричиняє, більшість вітчизняних підприємств не вживають жодних заходів щодо розслідування, недопущення чи попередження його виникнення.

4. Обґрунтовано, що актуалізація проблеми шахрайства в Україні є результатом поєднання двох чинників: складних умов ведення бізнесу, пов'язаних із воєнним станом, що посилюють невизначеність і послаблюють «імунітет» підприємств до протиправних дій шахрайського характеру; подальшого проникнення цифрових технологій, які створюють нові можливості для економічних шахраїв.

5. Дістало подальшого розвитку визначення сучасних причин корпоративного шахрайства в Україні. У результаті аналізу стану та динаміки розвитку вітчизняних підприємств виокремлено чинники, які опосередковано впливають на посилення ризиків виникнення шахрайства на підприємствах: зменшення кількості діючих підприємств, а отже, кількості зайнятих, падіння обсягів капітальних інвестицій, зниження фінансових можливостей підприємств для забезпечення економічної безпеки.

6. Аналіз сучасної системи економічного форензіку, яку значною мірою представляють консалтингові компанії «Великої аудиторської четвірки», дозволив окреслити практичну сферу застосування економічного форензіку (у тому числі цифрового), сформувати перелік основних послуг, пов'язаних з економічним форензіком, і розглянути етапи форензіку. Удосконалено визначення суб'єкта, об'єкта проведення форензік-аудиту, користувачів і результату форензіку. Запропоновано: додати до переліку суб'єктів аудиторські компанії, що надають послуги, пов'язані з економічним форензіком; розглядати як об'єкт усі бізнес-процеси (у тому числі закупівлі, систему підготовки фінансової звітності та ін.); додати до переліку користувачів результатів форензіку судові органи; доповнити перелік результатів виявленням фактів шахрайства, оцінкою збитків, ідентифікацією причетних осіб, рекомендаціями щодо усунення проблем, покращення системи внутрішнього контролю та запобігання аналогічним ситуаціям у майбутньому, оцінкою відповідних ризиків.

7. На основі критичного аналізу досліджень щодо основних напрямів форензіку виявлено некоректне віднесення деяких напрямів діяльності до форензіку (наприклад, захист інтересів у суді); перетинання окремих напрямів («виявлення фактів і розрахунок збитків від шахрайської діяльності з боку співробітників організації» є складовою «проведення незалежного фінансового розслідування як усередині організації, так і за її межами»); перенасичення тексту («визначення зовнішніх ризиків із використанням *публічних і непублічних* джерел інформації»); відсутність критеріїв оцінювання ефективності («оцінювання ефективності існуючих бізнес-процесів в організації»); плутанину у визначеннях (напрям – етап) тощо. У результаті систематизації досліджуваного матеріалу сформовано структуру системи економічного форензіку з позиції забезпечення економічної безпеки підприємств в Україні.

РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ІНСТИТУЦІЙНОГО МЕХАНІЗМУ ЕКОНОМІЧНОГО ФОРЕНЗІКУ В УКРАЇНІ

3.1 Концептуальні положення інституційного механізму економічного форензіку в Україні

Конкретизація концептуальних засад забезпечення економічної безпеки підприємств із залученням інструментів економічного форензіку та їх формалізація для застосування у практиці підтримки управлінських рішень на рівні підприємств, а також органами державної та місцевої влади потребує розроблення відповідного інституційного механізму, практичне впровадження якого стане основою використання економічного форензіку в управлінні підприємствами через інтеграцію інструментарію економічного форензіку в модель прийняття та контролю за реалізацією управлінських рішень на рівні організаційного та інформаційного забезпечення цих процесів.

Перед викладенням основних положень інституційного механізму форензіку, спрямованого на забезпечення економічної безпеки підприємств і держави, необхідно конкретизувати деякі терміни, які використовуватимуться в подальшому описі механізму.

Дія – будь-яка фактична дія або оформлене документами рішення, яке приймається уповноваженими особами на підприємстві та може містити ті чи інші ризики для економічної безпеки. До дій можуть належати укладання контрактів, наймання співробітників, відвантаження товару, перерахування коштів і практично будь-які операції, пов'язані з персоналом, товарно-матеріальними цінностями, грошима та іншими цінними активами.

Ризик – властивість дії (або бездіяльності), яка може спричинити негативні наслідки для підприємства (фінансові або репутаційні збитки, простої, втрата товарно-матеріальних цінностей тощо). Наприклад, укладання договору про продаж товару може бути пов'язане з ризиками неочікуваного зростання собівартості, несплати тощо. Ризик не є неминучою подією, а може реалізуватися з певною імовірністю (від >0 до 100%). Характерною ознакою ризику є наявність імовірності його реалізації, а також потенційного збитку, що може виникнути в разі його настання.

Інцидент – факт реалізації ризику. Наприклад, укладання договору з ненадійним покупцем пов'язане з низкою ризиків, які можуть не реалізуватися, і угода буде виконана належним чином. Однак у разі реалізації ризик вважається інцидентом (наприклад, несплата поставленого товару). Важливою характеристикою інциденту є сума фактичної шкоди, якої він завдав (але цю шкоду можна компенсувати при вживанні відповідних заходів).

Механізм – це процес поєднання інструментів і засобів, що підтримують його перебіг відповідно до певної мети. Отже, економічний механізм – це процес поєднання економічних інструментів і засобів, що підтримують його перебіг відповідно до певної мети. Мета не обов'язково має бути економічною – вона може перебувати в соціальній, демографічній або безпековій площині.

Термін «інституційний механізм» пов'язаний із державною політикою та державним управлінням, однак він є швидше науково-публіцистичним, ніж законодавчим (Федорчак, 2017). Найбільш поширеним підходом є його трактування як сукупності інститутів, що забезпечують належне безперебійне функціонування певної системи на основі легітимних правил, встановлених законодавством у певній сфері (Критенко & Даньшина, 2015), та набору певних правил і норм, а також організацій, що реалізують ці норми та правила на практиці (Кудрейко, 2014).

Інструменти економічного форензіку мають великий потенціал для сприяння економічній безпеці як окремих підприємств, так і держави загалом (цей потенціал охоплює як мікро-, так і макрорівні) за рахунок скорочення збитків від зловживань і ненавмисних помилкових дій співробітників та/або контрагентів. Проте наразі цей потенціал не використовується повною мірою не тільки на державному та регіональному рівнях, а й навіть на рівні підприємств. Цьому перешкоджає як непоінформованість щодо переваг даного інструментарію, так і відсутність єдиного механізму його застосування на мікро- та макрорівнях.

Традиційний економічний форензік дозволяє підприємствам набувати переваг на практиці, незважаючи на наявні недоліки, що не перешкоджають його застосовуванню як засобу забезпечення економічної безпеки на підприємстві на постійній основі. Зокрема, слід відзначити такі недоліки:

дискретний характер – дії аналізуються на предмет порушень чи ризиків уже за фактом настання інциденту чи завданих збитків або з певною періодичністю (раз на квартал або, наприклад, після закриття проєкту), а не на постійній основі;

домінуюча ручна обробка інформації – документи обробляються вручну (навіть якщо вони представлені в цифровому форматі), а результатом стають об'ємні звіти, опрацювання яких потребує значних часових і трудових ресурсів. Очевидно, що прискорення обробки та розширення охоплення інформацією потребуватимуть або радикального збільшення кількості залучених до обробки працівників, або використання засобів автоматизованої обробки інформації за мінімальною участю людини. Поширені системи на основі штучного інтелекту не замінюють діяльність професійних фахівців, а лише обмежено допомагають їм;

недостатня інтеграція в систему управління підприємством – відсутність безперервності, ручне опрацювання інформації та відсутність інтеграції на організаційному рівні не тільки не дозволяють вживати вчасних заходів, але і призводять до того, що економічний форензік використовується переважно як інструмент розслідування, а не підтримки прийняття управлінських рішень та запобігання інцидентам;

відсутність системного підходу на державному рівні – підприємства впроваджують інструменти форензіку за власною ініціативою без підтримки або керівництва з боку держави. У результаті немає єдиного розуміння економічного форензіку, охоплення впровадженням залишається низьким, а держава не набуває переваг, які потенційно могла б одержати у разі системного та масового застосування економічного форензіку на підприємствах.

Для подолання або обмеження негативного впливу зазначених недоліків необхідний системний підхід, заснований на таких принципах:

безперервність і максимальне охоплення дій (операцій) – дії аналізуються на предмет ризиків не за фактом настання інциденту і не з певною періодичністю, а вже в момент планування чи вчинення (за фактом внесення до електронної системи), що дозволяє розширити охоплення дій (в ідеалі – аналізувати всі дії), а отже, уможливлює виявлення ризиків і прискорення реагування на них;

використання сучасних цифрових технологій – безперервність і максимальне охоплення форензіком можливі лише за умови цифровізації процесів збору та обробки інформації з мінімізацією ручної праці та трудовитрат працівників. Інформація про дії має вноситися до електронної системи та оброблятися за допомогою автоматизованих процесів із використанням технологій блокчейн, машинного навчання та штучного інтелекту. Це означає перехід до цифрового форензіку;

інтеграція в практику управління підприємством – на відміну від класичних підходів, коли форензік використовується для виявлення інцидентів, що відбулися в минулому як реакція за фактом інциденту або як експертна підтримка при вирішенні спорів, запропонований підхід передбачає впровадження форензіку в систему управління шляхом своєчасного інформування осіб, які приймають рішення, про ризики тих чи інших дій, що здійснюються на підприємстві, та надання «дієвих» рекомендацій (в англомовній літературі – «actionable», тобто рекомендацій, на основі яких можна ухвалити управлінське рішення);

орієнтація на внутрішнє врегулювання інцидентів у межах підприємства – незважаючи на те що результати економічного форензіку можуть стати основою для звернення до правоохоронних органів як доказової бази, у значній частині випадків заподіяння економічної шкоди існує можливість врегулювання ситуації власними силами підприємства без залучення правоохоронних органів, зокрема шляхом взаємодії з причетними співробітниками та контрагентами. До того ж своєчасне виявлення ризиків дозволяє мінімізувати як імовірність їх реалізації, так і потенційні збитки в разі настання інцидентів. Основними мотивами застосування такого підходу є прагнення до оперативного врегулювання кризових ситуацій, а також оптимізація юридичних і репутаційних витрат, пов'язаних із залученням правоохоронних органів;

упровадження форензіку на інституційному рівні – сприяння впровадженню економічного форензіку та координація його використання на підприємствах через державні інститути дозволять перейти від фрагментарного впровадження за ініціативою окремих підприємств до системного застосування на основі єдиних стандартів, типових інструментів і загальних засобів звітності. Це уможливить набуття переваг як на рівні окремих підприємств (стандарти-

зація та полегшення процесів упровадження, доступ до інструментів), так і на рівні держави загалом (зокрема, за рахунок централізованого доступу до інформації по підприємствах, зниження навантаження на правоохоронні органи, збільшення податкових надходжень і загального поліпшення економічної ситуації).

З урахуванням вищезазначеного інституційний механізм економічного форензіку для забезпечення економічної безпеки підприємств і держави запропоновано трактувати як реалізовану на рівні підприємств та держави систему, що поєднує внутрішній взаємозв'язок і порядок здійснення процесів та процедур, а також їх методичне, організаційне, інформаційне, правове й ресурсне забезпечення, функціонування якої спрямоване на підвищення економічної безпеки підприємств і держави із застосуванням інструментів форензіку. Отже, цей механізм є способом інтеграції науково-методичних положень у практику управління на рівні підприємств і держави та має відображати порядок використання розроблених підходів у практиці управління, включаючи послідовність реалізації концептуальних основ економічного форензіку, вхідної та вихідної інформації, засобів обробки інформації, а також закріплення відповідних процесів за елементами організаційної структури на рівні підприємств і держави.

Як зазначено вище, для ефективного використання потенціалу економічного форензіку відповідний інституційний механізм має ґрунтуватися на системному впровадженні форензіку з максимальним охопленням підприємств; одержанні економічного ефекту як на рівні окремих підприємств, так і на регіональному та державному рівнях; створенні єдиного інформаційного простору шляхом централізованого збору на державному рівні інформації від окремих підприємств; використанні сучасного програмного інструментарію для збору та аналізу даних, а також для супроводу процесів реагування на виявлені проблеми та прийняття рішень, включаючи автоматизовані робочі місця, електронні сховища даних, інструменти штучного інтелекту, машинного навчання та ін.

Інституційний характер механізму проявлятиметься в тому, що впровадження економічного форензіку здійснюватиметься на рівні інститутів, тобто шляхом формування відповідних «правил гри», коли не просто окремі підприємства за власною ініціативою впроваджують економічний форензік для набуття відповідних

економічних переваг у вигляді зниження втрат, поліпшення керованості та підвищення економічної ефективності, але й держава стимулює впровадження економічного форензіку, щоб дістати таких переваг, як скорочення кількості випадків ухилення від сплати податків, підвищення ефективності економіки, зниження навантаження на правоохоронну та судову систему. Крім того, формування єдиної інформаційної системи, що забезпечує цілісне уявлення про фінансові порушення та заходи щодо їх протидії на рівні підприємств, створить передумови для прийняття більш ефективних рішень в економічній та правовій сферах.

Загальна суть запропонованого підходу полягає в об'єднанні двох рівнів: акумулювання даних і вживання заходів на рівні підприємств; державний доступ до агрегованих даних й упровадження загальнонаціональних чи галузевих заходів. Відмінність підходу від існуючих полягає в інтеграції економічного форензіку на рівні підприємства та місцевих/державних органів влади шляхом використання даних, зібраних та опрацьованих на рівні окремих підприємств, для прийняття рішень на державному рівні.

На рис. 3.1 наведено загальну схему економічного форензіку на підприємствах (у квадратних дужках зазначено джерела витрат й економічного ефекту), яка є універсальною та не залежить від конкретних інструментів чи організаційних форм (структур) його реалізації. У такій інтерпретації економічний форензік зводиться до аналізу дій з метою виявлення та мінімізації ризиків, а також швидкого реагування на інциденти.

Відправною точкою завжди є аналіз дій (як правило, здійснюється на основі первинних документів), за результатами якого в них можуть бути виявлені або не виявлені ознаки ризику. Якщо ознак ризику не виявлено, то заходи не вживаються, при цьому за фактом інциденти можуть статися (у такому випадку це свідчить про неефективність інструментів виявлення ризиків).

У разі виявлення ознак ризику може бути прийнято рішення про його мінімізацію (наприклад, якщо ризик пов'язаний із великими потенційними збитками) або про те, щоб не вживати жодних заходів (передбачається, що ризик не реалізується у зв'язку з його низькою імовірністю або шкода буде меншою за потенційні витрати на мінімізацію ризику).

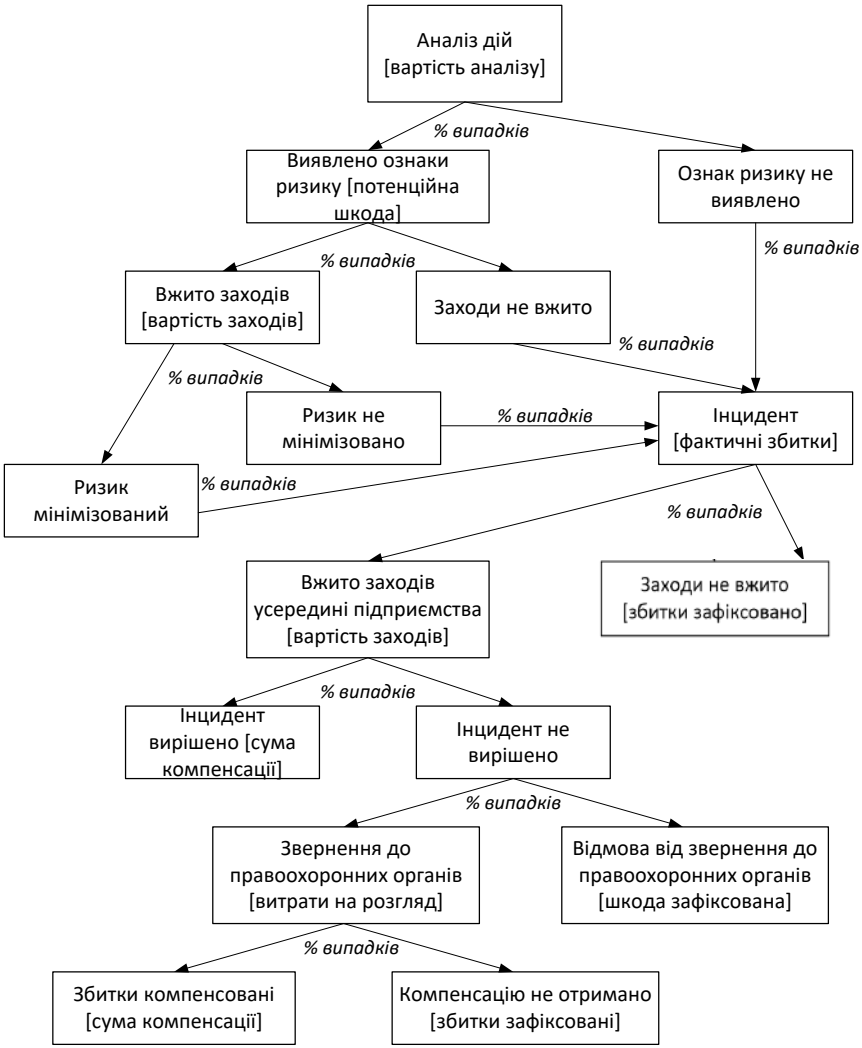

Рис. 3.1. **Загальний процес економічного форензіку на підприємствах**

Джерело: складено автором.

Заходи, вжиті для мінімізації ризику, можуть бути як успішними (ризик вдалося мінімізувати), так і невдалими (ризик не вда-

лося мінімізувати, незважаючи на витрачені ресурси). Кожному з таких випадків (успішних і невдалих заходів) відповідає своя імовірність настання інциденту, пов'язаного з ризиком (очевидно, що при успішній мінімізації ризику інцидент настає в меншій кількості випадків, ніж при невдалій спробі його мінімізації).

При настанні інциденту підприємство зазнає фактичної шкоди внаслідок реалізації ризику та може прийняти рішення про вживання заходів щодо компенсації цієї шкоди або відмовитися від таких заходів і зафіксувати шкоду. Наприклад, якщо відбулася закупівля сировини за завищеною ціною, то підприємство може або залишити ситуацію без змін, або спробувати вжити заходів щодо проведення розслідування з подальшою спробою компенсувати різницю між сплаченою та об'єктивною ринковою вартістю.

У разі прийняття рішення про вживання заходів на першому етапі вони реалізуються на підприємстві власними силами без залучення правоохоронних органів. За результатами цих заходів інцидент може бути врегульований з отриманням відповідної суми компенсації.

Якщо інцидент не вдається врегулювати самостійно, то підприємство може або звернутися до правоохоронних органів, або зафіксувати збитки.

За підсумками розгляду інциденту правоохоронними органами підприємство може або отримати компенсацію завданих збитків, або, в разі негативного результату, залишитися без компенсації.

Ефективність усіх описаних процесів може бути підвищена при реалізації економічного форензіку з використанням цифрових інструментів та в рамках єдиного механізму, визначеного вище. Інституційний механізм економічного форензіку для забезпечення економічної безпеки підприємств і держави включає два взаємопов’язаних рівні – мікро- та макро-.

На рис. 3.2 наведено елементи (структурні підрозділи, процеси, інструменти) забезпечення інституційного механізму економічного форензіку, які мають бути на окремих підприємствах.

Збір інформації. На першому етапі розгортання системи економічного форензіку на підприємстві впроваджується безперервний збір інформації, яка потенційно може використовуватися для виявлення небажаних дій, що можуть містити ризики економічної

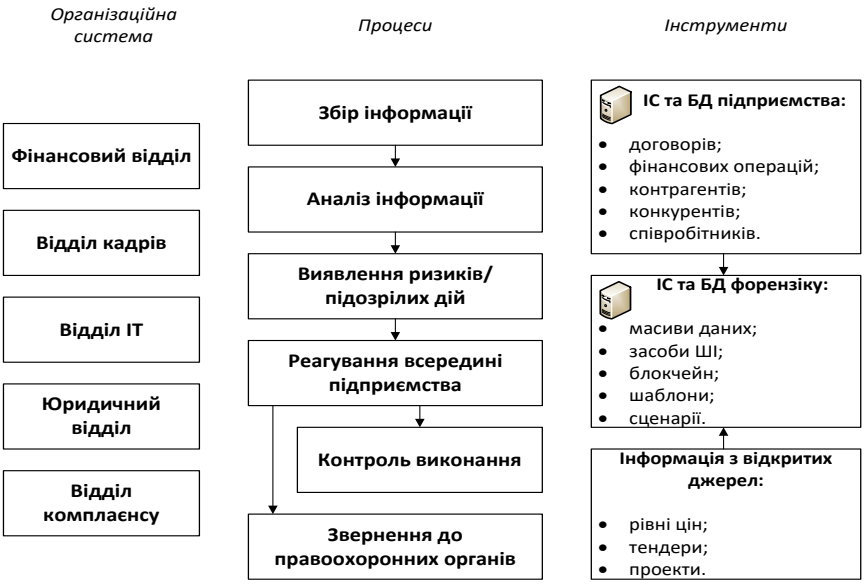

Рис. 3.2. **Елементи забезпечення інституційного механізму економічного форензіку на окремих підприємствах**
Джерело: складено автором.

безпеки. Це можуть бути дані про укладені договори, плановані або здійснені фінансові операції, а також про конкурентів, контрагентів і співробітників. Таку інформацію отримують з інформаційних систем і баз даних (ІС та БД), наявних на підприємстві. Також може використовуватися інформація з відкритих джерел (середній рівень цін, тендерні пропозиції, проєкти, що реалізуються тощо). Інформація може як вилучатися з існуючих систем і баз даних під час використання, так і зберігатися в окремій базі даних економічного форензіку. Основними критеріями є надійність зберігання та можливість отримання доступу в будь-який момент.

Аналіз інформації. Необхідно аналізувати інформацію як за стандартними метриками (наприклад, середні закупівельні ціни за договорами, середні ціни реалізації продукції та ін.), так і безпосередньо для виявлення підозрілих дій. Характер цих ознак визначається специфікою конкретної галузі, тому перевірки здійснюються фахівцями, які спеціалізуються у відповідній сфері. Також можливе

здійснення перевірок, рекомендованих сторонніми фахівцями, зовнішніми консультантами, державними органами та ін.

Наприклад, договори на закупівлю доцільно проаналізувати за такими потенційними підозрілими елементами:

відхилення цін від середньоринкових (біржових) цін або зафіксованих при реалізації аналогічних проєктів;

наявність фактичних і потенційних конфліктів інтересів (наприклад, споріднені відносини між співробітником підприємства та співробітником контрагента або коли відповідальна за затвердження договору особа є працівником підприємства-контрагента);

наявність підприємства-контрагента та його співробітників у санкційних списках, галузевих «чорних списках», базах даних судових рішень і виконавчих проваджень;

наявність інших підозрілих ознак, таких як розбіжність предмета договору та сфери діяльності контрагента, платежі готівкою, платежі до інших країн, використання ланцюжків посередників та ін.

У процесі аналізу інформації можна використовувати сучасні підходи до цифровізації процесу економічного форензіку на основі машинного навчання та штучного інтелекту, які дозволять, наприклад, надавати бальну оцінку потенційним ризикам, ґрунтуючись на низці контрольованих прямих чи непрямих ознак. Чим більше накопичиться вихідних даних, тим точнішими будуть оцінки таких інформаційних систем. Крім того, упровадження запропонованого інституційного механізму на державному рівні уможливлює створення єдиної бази даних економічного форензіку та досягнення максимальної точності виявлення ризиків і підозрілих випадків, прогнозування наслідків і вибору ефективних заходів реагування.

Виявлення ризиків / підозрілих дій. Описаний аналіз виконується з метою виявлення ризиків/підозрілих дій. Інформаційна система надає повідомлення про потенційні проблеми, супроводжуючи їх автоматично сформованими аналітичними матеріалами (такими як коротке зведення вихідних даних, бальна оцінка ризиків, перелік задіяних відділів і співробітників та ін.), однак рішення про те, чи є конкретна дія або подія ризиком / підозрілою дією або навіть фактичним порушенням, приймає профільний співробітник. Це може бути начальник відділу, у якому зафіксовано таку дію, начальник відділу комплаєнсу (нормативно-правової відповідності) або

юридичного відділу. Якщо неприйнятність і загрозливий характер дії підтверджено, то подія передається на рівень реагування в межах підприємства. Дуже важливим аспектом є фіксація інформації як про підтверджені випадки, так і про ті, що не підтвердилися, в інформаційній системі економічного форензіку, оскільки це необхідно для навчання системи та збільшення ймовірності правильної класифікації ситуації при виникненні подібних випадків у майбутньому.

Реагування в межах підприємства. У більшості випадків, за умови вчасного виявлення, ризики можуть бути локалізовані та мінімізовані на рівні підприємства без значної фінансової та репутаційної шкоди та без залучення правоохоронних органів. У процесі реагування можуть брати участь відділи (або інші структурні підрозділи, наприклад, департаменти, управління та ін.), у яких відбулося порушення, а також юридичний відділ або відділ комплаєнсу. Окрім прямого розгляду порушень, може застосовуватися процес медіації (за посередництва нейтральної особи, яка прагне зрозуміти й урахувати інтереси всіх учасників події). За потреби можуть залучатися незалежні експерти у конкретній галузі. У разі підтвердження порушення в ідеальній ситуації порушник після пред'явлення доказів усвідомлює свої дії, виправляє порушення (наприклад, скасовує контракт, укладений за завищеними цінами) та компенсує завданий підприємству збиток (повертає суму переплати, якщо суму за контрактом уже було виплачено). Також до порушника можуть застосовуватися внутрішні службові стягнення (догана, переведення на нижчу посаду тощо).

Контроль за виконанням. Якщо за результатами реагування було прийнято рішення про реалізацію тих чи інших заходів, то необхідно проконтролювати їх виконання. З точки зору формування бази даних і навчання інформаційної системи форензіку, контроль за виконанням є важливим, оскільки на цьому етапі надходять дані про отримані (повернені) в результаті реалізації заходів кошти. Ці дані дозволяють розрахувати економічний ефект від витрат на функціонування системи, імовірність компенсації збитків у тих чи інших ситуаціях, терміни компенсації збитків, а також одержати іншу інформацію, яка надалі може використовуватися для прийняття управлінських рішень на підприємстві, а в разі створення інтегрованої національної системи –на регіональному та державному рівнях.

Залучення правоохоронних органів і судової системи. Якщо керівництво підприємства та особи, відповідальні за управління ризиками економічної безпеки підприємства, не змогли вирішити проблему шляхом переговорів, медіації чи інших внутрішньокорпоративних заходів, то підприємство звертається до правоохоронних органів або до суду з метою компенсації втрат і притягнення порушників до відповідальності. Такі дії можуть стосуватися як співробітників підприємства, так і контрагентів (наприклад, у разі змови з метою завищення цін). Дані за результатами таких розглядів також фіксуються в інформаційній системі економічного форензіку на рівні підприємства, а потім використовуються для формування звітів, навчання системи тощо. З урахуванням наявності єдиного державного реєстру судових рішень можливим є експорт необхідної інформації в режимі онлайн.

У функціонуванні системи економічного форензіку можуть бути задіяні такі відділи підприємства:

фінансовий (економічний) – фіксує дані про фінансові транзакції в інформаційних системах (включаючи інформаційну систему економічного форензіку), аналізує фінансові операції, надає висновок про рівень ризику тих чи інших фінансових операцій, аналізує дані з відкритих джерел (рівні цін, конкуренти, контрагенти);

відділ кадрів – вводить дані про співробітників до інформаційних систем (включаючи інформаційну систему економічного форензіку), здійснює моніторинг сімейних і ділових зв'язків чинних та потенційних працівників на предмет конфліктів інтересів;

відділ ІТ – забезпечує впровадження інформаційної системи форензіку, мережевої інфраструктури та баз даних, автоматизований збір інформації з відкритих джерел, інтеграцію технологій ШІ, машинного навчання та блокчейну в інформаційну систему економічного форензіку, обмін інформацією між відділами;

юридичний – здійснює підготовку договорів, аналізує юридичні наслідки ризиків і порушень, бере участь у внутрішньому врегулюванні виявлених порушень, готує матеріали та супроводжує юридичні дії чи розслідування в разі їх виходу за межі підприємства (розслідування правоохоронними органами, судові позови);

відділ комплаєнсу – здійснює моніторинг законів, правил і стандартів, контролює їх виконання підприємством, здійснює навчання персоналу у сфері нормативно-правових вимог, у випереджальному порядку виявляє, документує та аналізує ризики, у

тому числі встановлення нових видів господарських і клієнтських відносин чи суттєві зміни в їх характері.

Крім того, у функціонуванні системи економічного форензіку можуть брати участь інші відділи, пов'язані з конкретною сферою ризиків (виробничий відділ, відділ заробітної плати та винагород, складські служби, закупівельні підрозділи та ін.), керівництво підприємства, вищі корпоративні служби (за наявності таких) та ін.

Слід зазначити, що на практиці юридичний відділ і відділ комплаєнсу можуть бути або різними відділами, або одним. При роздільному форматі юридичний відділ може відповідати за консультування керівництва про закони, правила та стандарти, що стосуються управління ризиками, і за складання інструкцій для працівників, тоді як відділ комплаєнсу може відповідати за контроль за дотриманням політик і процедур, звітність перед керівництвом.

Дані, які вносяться до внутрішньокорпоративної системи економічного форензіку, консолідуються за п’ятьма групами: внутрішньокорпоративні дані; інформація з відкритих джерел; інформація про конкретні випадки; інформація про вжиті внутрішні заходи та їх результати; інформація про звернення до правоохоронних органів та їх результати (табл. 3.1).

Таблиця 3.1. **Дані, які фіксуються у внутрішньокорпоративній системі економічного форензіку**

Група даних	Дані
1. Внутрішньокорпоративні	Дані про співробітників, контрагентів, конкурентів, фінансові операції
2. Інформація з відкритих джерел	Дані про рівні цін, конкурентів, тендери, а також про сферу діяльності підприємства та його оточення
3. Інформація про конкретні випадки	Задіяні особи, операції, суми, контрагенти, наслідки, час та обставини
4. Інформація про вжиті внутрішні заходи та їх результати	Характер заходів, задіяні особи, терміни, зазнані витрати, відповідальні за реалізацію, попереджені або компенсовані збитки
5. Інформація про результати залучення правоохоронних органів	Задіяні органи, учасники з боку підприємства, терміни розгляду, результати, зазнані витрати, попереджені або компенсовані збитки

Джерело: складено автором.

У сучасних умовах, що характеризуються подальшим поглибленням цифровізації, функціонування системи економічного форензіку є неможливим без застосування відповідних програмних засобів і технологій, зокрема:

інформаційна система – уможливлює внесення, доступ, аналіз та візуалізацію інформації в зручному вигляді у форматі автоматизованих робочих місць (як стаціонарних із використанням ПК, так і мобільних із використанням смартфонів, планшетів). Співробітники взаємодіють із системою економічного форензіку насамперед через інформаційну систему відповідно до своїх прав доступу із застосуванням інформаційних панелей, форм введення даних, попереджень та інших елементів інтерфейсу;

бази даних – забезпечують внесення, зберігання та доступ до повного масиву інформації, що використовується у процесі економічного форензіку, у тому числі бази даних фінансових операцій, договорів, співробітників, контрагентів і конкурентів, ризиків, інцидентів, інформації з відкритих джерел тощо;

засоби автоматизованої обробки інформації, у тому числі машинне навчання, ШІ та блокчейн – в інформаційну систему інтегруються механізми автоматизованої обробки інформації, з використанням яких аналізуються операції на основі встановлених характеристик та оцінюється ризик (бальна оцінка, «червоні прапорці», попередження тощо). Окрім іншого, оцінка може виконуватися на основі алгоритмів («якщо-то») або нейромереж (коли мережа навчається на основі наявних даних щодо операцій: є масив даних щодо операцій і є випадки, коли операції дійсно завдали шкоди, – при достатньо великій вибірці нейромережа дозволяє з високою імовірністю відносити операції до ризикованих з урахуванням явних та неявних ознак).

Алгоритм використання інструментарію економічного форензіку на підприємстві в аспекті супроводу конкретних процесів (економічних операцій) представлено на рис. 3.3.

Першим етапом завжди є прийняття уповноваженими особами того чи іншого рішення, що оформлюється у вигляді документа. Для цифрової системи економічного форензіку документ повинен мати електронну форму. У разі функціонування на підприємстві повністю електронного документообігу первинний документ оформлюється безпосередньо в системі електронного документообігу. Якщо ж з певних причин документ було створено в паперовій формі, то він підлягає внесенню до відповідної електронної системи.

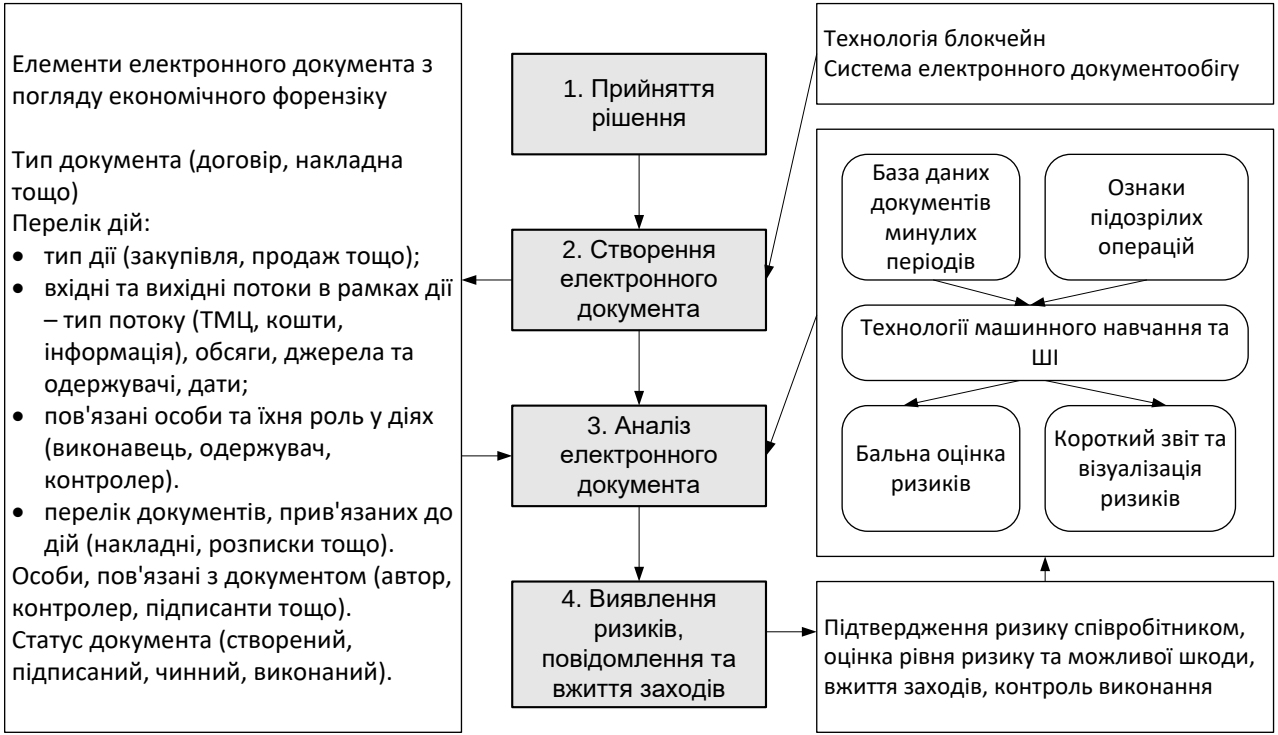

Рис. 3.3. **Функціонування системи форензіку при супроводі конкретних операцій**
Джерело: складено автором.

Щоб унеможливити викривлення документів, їх зміну з датою, що відрізняється від фактичної дати створення документа, або оформлення без згоди зазначених у ньому осіб, доцільно використовувати систему електронного документообігу з технологією блокчейн. Також блокчейн можна застосовувати і для забезпечення цілісності даних в інформаційній системі форензіку подібно до використання в системах Інтернету речей (підключеного до мережі обладнання) (Akinbi et al., 2022).

Автоматизований аналіз документів виконується не у вигляді вихідного тексту, а за виокремленими в ньому елементами (атрибутами). При цьому ідентифікація та введення атрибутів у систему можуть здійснюватися як вручну, так і з використанням технологій на основі ШІ. У будь-якому разі вхідним масивом даних для економічного форензіку є сукупність елементів документа, що відображають суть передбачуваної ним дії, її економічні наслідки та задіяних осіб. Крім стандартних для всіх документів атрибутів, таких як тип документа, автори, підписанти, терміни виконання та ін., специфічні ключові елементи для аналізу включають перелік дій, передбачених у процесі виконання документа. Виокремлено такі характеристики кожної дії:

тип (закупівля, продаж та ін.);

вхідні та вихідні потоки в рамках дії – тип потоку (товарно-матеріальні цінності, кошти, інформація), обсяги, джерела та одержувачі, дати планового та фактичного переміщення потоків;

пов'язані особи та їх роль у дії (виконавець, одержувач, контролер);

перелік документів, пов’язаних із виконанням дії (накладні, розписки тощо);

особи, пов'язані з документом (автор, контролер, підписанти та ін.).

Наприклад, якщо документ передбачає закупівлю сировини, то в процесі економічного форензіку аналізуються планові та фактичні вхідні й вихідні фінансові потоки, потоки товарно-матеріальних цінностей, ціни на сировину, обсяги та строки поставки, пов'язані юридичні та фізичні особи (на предмет їх зв'язку з конкурентами, історії правопорушень, корупційних зв'язків тощо), правильність оформлення супутніх документів тощо.

Аналіз може виконуватися як у ручному, так і в автоматизованому режимі. Перевагами автоматизованої обробки є швидкість і

можливість охопити великі обсяги документів із залученням мінімальних людських ресурсів. Такий автоматичний аналіз доцільно здійснювати з використанням технологій машинного навчання та ШІ – на основі даних проаналізованих у минулому документів (масиви атрибутів документів та відповідних їм підтверджених відомостей про порушення та ризики), а також введених вручну ознак підозрілих операцій ШІ. Чим більше даних внесено до системи, тим точніше працюватиме навчена система.

Остаточне рішення про те, чи підтверджено ризик, залишається за співробітником, якому система надає всю необхідну інформацію. Після виявлення ризику виконуються стандартні дії щодо повідомлення відповідальних осіб і в системі економічного форензіку фіксується їх реакція, що дозволяє підвищити ефективність оцінювання ризиків у майбутньому.

Існує багато способів пошуку слідів порушень або протиправної діяльності в цифровому середовищі, зокрема: аналіз ознак шахрайства в документах, облік фактичних або потенційних шахраїв серед контрагентів, створення баз даних шахрайських документів (Ribaux et al., 2022). Існують різні моделі автоматизованого виявлення повторюваних закономірностей (патернів) у процесі цифрового форензіку шляхом аналізу окремих часових рядів формально незалежних подій (Galbraith et al., 2020).

Подібні методи можуть використовуватися в цифровій автоматизованій системі економічного форензіку на підприємствах.

Розгорнута відповідно до вищевикладених положень система економічного форензіку на підприємстві забезпечує:

систематичний збір інформації, пов'язаної з потенційними ризиками економічної безпеки, із використанням внутрішньокорпоративних інформаційних систем;

аналіз операцій щодо ризиків економічної безпеки з використанням засобів автоматизованої обробки інформації (включаючи ШІ) та повідомлення відповідальних осіб;

розгляд виявлених ризиків та, за необхідності, вживання заходів як на рівні підприємства, так і (за необхідності) із залученням правоохоронних органів;

оцінку економічної ефективності системи економічного форензіку шляхом контролю витрат на її функціонування, запобігання збиткам та/або отриманим сумам компенсації;

передачу інформації (про виявлені ризики, виявлені порушення, запобігання шкоді, ефективність системи тощо) на державний рівень з метою подальшого аналізу та вдосконалення державної політики.

Система економічного форензіку створює можливості виявлення та реагування на економічні ризики в межах підприємства, проте її інституційна реалізація на державному рівні дозволяє дістати додаткових переваг (підрозділ 3.3).

Застосування запропонованого інституційного механізму форензіку посилює економічну безпеку як у межах конкретного підприємства, так і на рівні держави загалом. Переваги на рівні підприємства полягають у такому:

забезпечення систематизованого збору й аналізу інформації про господарські операції, які можуть становити ризик для економічної безпеки підприємства;

підвищення дисципліни працівників за рахунок покращення контролю за їхніми діями та їх поінформованості про такий контроль;

організація роботи у стандартизованому форматі з використанням програмних засобів із зручним інтерфейсом;

автоматизоване виявлення ризиків і надання попереджень керівництву підприємства;

можливість запобігання збиткам або їх компенсації на ранніх етапах, поки вони ще не набули незворотного характеру;

можливість врегулювання кризової ситуації без залучення правоохоронних органів, а також без відповідних витрат та шкоди репутації;

постійне підвищення якості виявлення та класифікації ризиків за рахунок використання інструментів машинного навчання, ШІ та блокчейну;

оцінювання економічної ефективності заходів, спрямованих на запобігання збиткам, медіацію, мінімізацію ризиків тощо.

Оскільки система економічного форензіку наразі практично не застосовується на вітчизняних підприємствах, її впровадження стане інновацією для більшості з них.

Запропоновано реалізувати механізм на інституційному рівні – поєднати застосування економічного форензіку на окремих підприємствах з удосконаленням державної політики на основі систе-

матизації та уніфікації процесів упровадження та використання на державному рівні інформації з корпоративних систем форензіку, зокрема з метою відповідної модернізації нормативно-правової бази в цій сфері. Розроблений механізм передбачає активне застосування сучасних інформаційних технологій, у тому числі блокчейн і ШІ.

3.2 Економічний ефект від упровадження інституційного механізму економічного форензіку

Цифровий економічний форензік може забезпечити для підприємства одержання переваг, частину з яких можна безпосередньо виміряти з позиції фінансової вигоди. Інша частина має нефінансовий характер, проявляється в поліпшенні діяльності підприємства загалом, але також обумовлює економічні переваги в довгостроковій перспективі, які, однак, складно або неможливо виміряти безпосередньо. Економічний ефект досягається за рахунок попередження і компенсації збитків, спричинених помилковими чи протиправними діями. Основне джерело статистичної інформації, яка є узагальненою та аналізується лише в агрегованій формі, становлять звіти правоохоронних органів, зокрема Генеральної прокуратури (Мельничук, 2021).

Однак більшість епізодів залишається поза увагою правоохоронних органів, тому що підприємства віддають перевагу врегулюванню деяких проблемних ситуацій власними силами. Бюро економічної безпеки (БЕБ) у своїх звітах (Бюро економічної безпеки, 2024) обмежується зведеними даними та не публікує інформацію про методи, які воно використовує для оцінювання економічного ефекту, а лише наводить конкретні сфери попередження протиправних дій («зупинено незаконне відшкодування ПДВ», «упереджено розповсюдження ризикового податкового кредиту з ПДВ», «упереджено розкрадання під час закупівель» тощо) без зазначення конкретних розрахунків.

Оскільки в процесі аналізу здійснених раніше досліджень не виявлено достатньо обґрунтованих підходів до комплексного оцінювання економічного ефекту на рівні підприємства від упровадження економічного форензіку, актуальним є розроблення підходу, який би комплексно враховував ефект від попередження

небажаних ситуацій чи компенсації збитків як власними силами підприємства, так і із залученням правоохоронних органів, витрати на впровадження інструментарію та інші важливі чинники.

Основні переваги економічного форензіку для підприємства полягають у такому:

мінімізація фінансових збитків. Економічний форензік допомагає оперативно виявляти інциденти у сфері економічної безпеки та вживати відповідних заходів, знижуючи ризик фінансових втрат. Вчасне виявлення та реагування можуть запобігти ризикам або мінімізувати їхні наслідки;

мінімізація витрат, пов'язаних із залученням правоохоронних органів. Вчасне виявлення ризиків, інцидентів та їх врегулювання на рівні підприємства без залучення правоохоронних органів забезпечують економію судових витрат, а також на підготовці скарг і позовів, проведенні експертиз, необхідності відволікання працівників від основної діяльності для участі в розслідуваннях тощо;

дотримання законодавства. Дотримання законодавчих і нормативних вимог має велике значення для бізнесу з позицій забезпечення його безперервної діяльності. Економічний форензік допомагає запобігати порушенням законодавства та збирати докази з метою подальшого використання в юридичних процедурах, забезпечуючи дотримання підприємством відповідних законів і правил, що сприяє уникненню дорогих судових позовів і штрафів;

захист інтелектуальної власності. Підприємства вкладають значні кошти в розвиток інтелектуальної власності, а економічний форензік допомагає захистити ці активи, виявляючи та усуваючи порушення безпеки чи події, які можуть поставити під загрозу конфіденційну інформацію, комерційну таємницю чи конфіденційні дані;

скорочення витрат на реагування на ризики. Налагоджений процес цифрового форензіку забезпечує більш швидке й ефективне реагування на ризики. Це дозволяє знизити загальні витрати, пов'язані з розслідуванням та усуненням ризиків для економічної безпеки, а також звести до мінімуму негативний вплив на діяльність підприємства;

поліпшення репутації. Громадська думка відіграє важливу роль у діяльності багатьох підприємств. Економічний форензік

допомагає запобігати ризикам економічної безпеки та мінімізувати їх наслідки, захищаючи репутацію організації. Швидке та прозоре реагування на інциденти сприяє відновленню довіри клієнтів, партнерів і зацікавлених сторін;

зниження обсягу страхових премій. Упровадження ефективних методів економічного форензіку може призвести до зниження обсягу страхових премій при страхуванні від фінансових втрат, кіберзагроз, судових процесів тощо. Страхові компанії схильні стимулювати підприємства, які мають надійні заходи безпеки та плани реагування на інциденти, шляхом надання більш вигідних умов страхування;

запобігання простоям і перебоям у діяльності. Економічний форензік не лише спрямований на виявлення та запобігання ризикам, але і сприяє розробленню надійних планів забезпечення безперервності діяльності та екстреного відновлення. У разі виникнення ризиків економічної безпеки або фактичних інцидентів наявність чітко визначених процесів може скоротити час простоїв та пов'язані з ними фінансові втрати;

посилення довіри постачальників і партнерів. Більшість підприємств у своїй діяльності залежать від мережі постачальників і партнерів. Демонстрація прихильності до забезпечення економічної безпеки за допомогою впровадження заходів економічного форензіку може підвищити довіру до підприємства та зміцнити ділові відносини;

зростання продуктивності праці співробітників. Інструменти та процеси економічного форензіку можуть допомогти в моніторингу та управлінні діяльністю співробітників і підвищити загальну продуктивність праці за рахунок зниження ризиків неправомірної корисливої поведінки, порушень дисципліни, недбалого ставлення до дотримання вимог захисту конфіденційності й інтелектуальної власності тощо;

конкурентні переваги. Здатність продемонструвати високий рівень економічної безпеки як самого підприємства, так і його партнерів, а також ефективні можливості економічного форензіку можуть виокремити підприємство на тлі конкурентів, оскільки замовники та партнери здебільшого віддають перевагу співробітництву з організаціями, для яких питання економічної безпеки та інвестиції в надійні засоби й інструменти є пріоритетними.

Таким чином, економічний форензік на підприємстві сприяє підвищенню безпеки та стійкості його діяльності, допомагаючи захистити фінансові ресурси й інтелектуальну власність, забезпечити дотримання законодавства та підвищити загальну ділову репутацію, конкурентоспроможність. Проте оцінювання економічної ефективності реалізації таких заходів і використання відповідних інструментів ускладнюється тим, що лише частина з них спрямовані на запобігання безпосередньому фінансовому збитку або скорочення витрат, у той час як інші мають непрямий ефект.

Системне впровадження інструментів економічного форензіку на підприємствах, а також реалізація відповідного інституційного механізму на рівні держави (насамперед, централізоване отримання від підприємств інформації про функціонування інструментів економічного форензіку та вдосконалення за результатами аналізу цієї інформації інституційних умов і нормативно-правового регулювання) можуть мати економічний ефект не лише на рівні окремого підприємства, але і на рівні держави.

Основними джерелами економічного ефекту є такі:

зниження навантаження на систему правоохоронних органів. Економічний форензік може знизити навантаження на правоохоронні органи як шляхом урегулювання подій у межах підприємства без їх залучення, так і через надання спеціалізованого висновку щодо встановлення факту вчинення фінансового злочину. Це дозволяє швидше й ефективніше розкривати економічні правопорушення та завершувати судовий розгляд справ, що забезпечує пряму економію бюджетних коштів і вивільняє ресурси правоохоронних органів для боротьби з іншою злочинною діяльністю;

поліпшення економічних показників підприємства шляхом зниження обсягу шкоди. Завдяки попередженню, виявленню, розслідуванню та запобіганню ризикам цифровий економічний форензік допомагає підприємству скоротити фінансові втрати, пов'язані з шахрайством, розкраданням та іншою незаконною діяльністю. Мінімізація таких збитків дозволяє підприємству підтримувати фінансову стабільність, цільові економічні показники, а також довіру інвесторів;

збільшення податкових надходжень за рахунок зменшення збитків для підприємств. Економічний форензік запобігає збиткам від ризиків економічної безпеки та скорочує їх, що, у свою

чергу, підвищує їхню здатність генерувати оподатковуваний дохід. Мінімізуючи наслідки помилкової або корисливої поведінки працівників, таких як завищення закупівельних цін, а також економічних злочинів, таких як фінансове шахрайство, економічний форензік опосередковано сприяє збільшенню податкових надходжень;

скорочення кількості інцидентів у сфері інтелектуальної власності та обробки персональних даних. Економічний форензік відіграє превентивну роль, сприяючи виявленню ризиків у процесі аналізу конкретних операцій і навіть загальних вразливостей у системах інтелектуальної власності та обробки персональних даних. Цей запобіжний підхід допомагає організаціям упроваджувати заходи безпеки, щоб знизити ймовірність настання подій, пов'язаних із витоком даних або крадіжкою інтелектуальної власності, тим самим захищаючи цінні активи – як власні, так і підприємств-контрагентів;

зниження рівня економічної злочинності. Застосування методів економічного форензіку сприяє виявленню, запобіганню й усуненню наслідків фінансових порушень, шахрайства та корупції. Економічний форензік відіграє роль стримувального чинника, який перешкоджає незаконним діям співробітників конкретних підприємств, що в масштабі економіки загалом веде до зниження рівня економічної злочинності;

загальне поліпшення економічної ситуації. Кумулятивний ефект зниження економічної злочинності, підвищення ефективності діяльності підприємств та збільшення обсягу податкових надходжень сприяють загальному поліпшенню економічної ситуації в країні. Економічний форензік, формуючи передумови для створення більш безпечного та прозорого економічного середовища, підтримує економічне зростання, ділову впевненість і загальне фінансове благополуччя.

На рис. 3.4 наведено загальну каузальну схему отримання економічного ефекту від економічного форензіку, включаючи джерела економічного ефекту на рівні окремого підприємства (звичайним шрифтом) та держави загалом (курсивом).

На рисунку можна побачити, як переваги економічного форензіку дозволяють отримати вимірний економічний ефект на рівні підприємства, а також приводять до переваг й економічного ефекту для держави загалом: скорочення витрат підприємств покращує їхні

Рис. 3.4. **Каузальна схема отримання економічного ефекту від економічного форензіку на рівні підприємства та держави**

Джерело: складено автором.

економічні показники, збільшуючи базу оподаткування та податкові надходження. Зменшення кількості звернень до правоохоронних органів приносить прямий економічний ефект як для окремого підприємства, так і для держави загалом (через потенціал зменшення видатків на правоохоронну систему), а посилення можливостей дотримання нормативно-правових вимог на підприємствах знижує загальний рівень економічної злочинності й інцидентів у сфері захисту інтелектуальної власності та персональних даних. Усе це зрештою зумовлює поліпшення загальної економічної ситуації.

У табл. 3.2 надано оцінку складності прямого розрахунку економічного ефекту від конкретних переваг економічного форензіку на рівні підприємств і держави загалом.

У подальшому запропоновано інструментарій і виконано оцінку ефекту економічного форензіку за перевагами, для яких можливий прямий розрахунок («низька складність» згідно з класифікацією в табл. 3.2) і будуть надані загальні рекомендації для переваг із «середньою» складністю розрахунку економічного ефекту. Переваги з «високою» складністю не оцінюватимуться, оскільки вони потребують масштабних наукових і практичних досліджень, що виходять за межі цієї роботи. Таким чином, на рівні підприємств буде виконано розрахунок економічного ефекту від запобігання фінансовим збиткам і витратам, пов'язаним із залученням правоохоронних органів, а також від скорочення витрат на реагування на ризики. На державному рівні – від зниження навантаження на правоохоронні органи та поліпшення економічних показників підприємств за рахунок зменшення збитків.

1. Розрахунок економічного ефекту за наявності «повних даних».

На початковому етапі доцільно розглянути розрахунок фактичного економічного ефекту за умови «повних даних», коли на підприємстві є інформація щодо кожного ризику, у тому числі реалізованих ризиків (інцидентів). Немає необхідності оперувати ймовірністю настання тих чи інших подій – усі розрахунки можна виконати з використанням методу прямого рахунку на основі доступної інформації (наприклад, інформаційної системи форензіку).

Таблиця 3.2. **Оцінка складності розрахунку економічного ефекту (ЕЕ) від переваг економічного форензіку**

№ з /п	Перевага	Ступінь складності розрахунку
1	2	3
1.	*Рівень підприємств*	
1.1	Мінімізація фінансових збитків	*Низька складність* – ЕЕ може бути розрахований безпосередньо як сума збитків, яким вдалося запобігти, за конкретними мінімізованими та викоріненими ризиками або отриманою компенсацією
1.2	Мінімізація витрат, пов'язаних із залученням правоохоронних органів	*Низька складність* – ЕЕ може бути розрахований безпосередньо як різниця між витратами на залучення правоохоронних органів і витратами на заходи в рамках економічного форензіку
1.3	Дотримання законодавства	*Середня складність* – для розрахунку ЕЕ необхідно знати конкретні збитки, що випливають із порушення законодавства, а також виміряти конкретний вплив економічного форензіку на кількість порушень
1.4	Захист інтелектуальної власності	*Середня складність* – розрахунок ЕЕ потребує інформації про потенційні збитки від порушень прав інтелектуальної власності
1.5	Скорочення витрат на реагування на ризики	*Низька складність* – ЕЕ розраховується як різниця у витратах на аналогічні заходи з використанням інструментарію економічного форензіку та без нього
1.6	Поліпшення репутації	*Висока складність* – розрахунок фінансового еквівалента репутації є окремим нетривіальним завданням
1.7	Зниження обсягу страхових премій	*Низька складність,* але здійсненність не залежить від самого підприємства – інформацію про зниження обсягу страхових премій може надати лише страхова компанія з урахуванням ситуації на ринку страхових послуг і перестрахування
1.8	Запобігання простоям і перебоям у діяльності	*Середня складність* – розрахунок ЕЕ можливий лише для ризиків, що призводять до простою
1.9	Посилення довіри постачальників і партнерів	*Висока складність* – оцінка рівня довіри та її впливу на схильність контрагентів до співпраці є окремим нетривіальним завданням

Закінчення табл. 3.2

1	2	3
1.10	Зростання продуктивності праці співробітників	*Висока складність* – розрахунок ЕЕ потребує виокремлення впливу економічного форензіку із сукупного впливу всіх чинників продуктивності праці
1.11	Конкурентні переваги	*Висока складність* – оцінка впливу економічного форензіку на конкурентоспроможність підприємства потребує вирішення окремого науково-практичного завдання
2	*Рівень держави*	
2.1	Зниження навантаження на правоохоронні органи	*Низька складність* – ЕЕ розраховується як пряма економія витрат унаслідок скорочення кількості звернень
2.2	Поліпшення економічних показників підприємств шляхом зниження збитків	*Низька складність* – ЕЕ може бути розрахований безпосередньо як сума шкоди, якої вдалося уникнути, по всіх підприємствах, на яких упроваджено економічний форензік
2.3	Збільшення податкових надходжень за рахунок зменшення збитків підприємств	*Середня складність* – для розрахунку ЕЕ необхідно точно визначити, як запобігання завдяки форензіку економічним збиткам впливає на базу оподаткування
2.4	Скорочення кількості негативних подій у сфері інтелектуальної власності та обробки персональних даних	*Висока складність* – розрахунок ЕЕ ускладнюється тим, що вплив форензіку на захист інтелектуальної власності та персональних даних є опосередкованим
2.5	Зниження рівня економічної злочинності	*Висока складність* – для розрахунку ЕЕ необхідно надати обґрунтовану числову оцінку впливу форензіку на рівень економічної злочинності
2.6	Загальне поліпшення економічної ситуації	*Висока складність* – необхідні обґрунтовані методи оцінювання зміни економічної ситуації та впливу окремих переваг форензіку на конкретні її аспекти, що потребує здійснення масштабних економічних досліджень

Джерело: складено автором.

Формула розрахунку економічного ефекту від **мінімізації фінансових збитків** на рівні підприємства:

$$EE_{dp} = \sum_{i=1}^{I}\left(L_{p,i} - L_{f,i} - C_i\right) - S\ ,$$

де EE_{dp}– загальний економічний ефект від мінімізації фінансових збитків за всіма ризиками;

I – загальна кількість ризиків, що підтвердилися, за певний період;

$L_{p,i}$ – потенційні збитки від *i*-го ризику;

$L_{f,i}$ – фактично завдані збитки від *i*-го ризику;

C_i – фактичні витрати на мінімізацію *i*-го ризику, у тому числі на проведення розслідування в межах підприємства та вживання відповідних заходів реагування;

S – сумарні витрати на функціонування системи економічного форензіку за аналізований період. Якщо економічний ефект розраховується відразу за кількома перевагами, то ці витрати віднімаються лише один раз (із суми економічного ефекту за всіма перевагами).

Для використання цього підходу до розрахунку економічного ефекту необхідно для кожного виявленого ризику визначити потенційну шкоду, яка була б завдана, якби ризик не був виявлений і не було б вжито заходів, фактичні збитки після вживання заходів (у кращому випадку вони можуть дорівнювати 0) і витрати на запобігання для даного конкретного ризику.

Формула розрахунку економічного ефекту на рівні підприємства від **запобігання витрат, пов'язаних із залученням правоохоронних органів**:

$$EE_{le} = \sum_{i=1}^{I}(a_i K_i - b_i C_i) - S\ ,$$

де EE_{le}– загальний економічний ефект від запобігання витратам, пов'язаним із залученням правоохоронних органів;

a_i– оператор, який вказує на те, чи була ситуація врегульована в межах підприємства замість звернення до правоохоронних органів, може набувати значення 0 (ні) або 1 (так);

b_i – оператор, який вказує на те, чи була здійснена спроба врегулювати ситуацію в межах підприємства замість звернення до правоохоронних органів (і зазнано відповідних витрат), може набувати значення 0 (ні) або 1 (так);

K_i – потенційні чи фактичні витрати в разі залучення правоохоронних органів стосовно *i*-го ризику.

Для розрахунків необхідно мати перелік ризиків або ситуацій, за якими були здійснені спроби внутрішнього врегулювання, і тих, за якими в результаті довелося звернутися до правоохоронних органів, а також витрати на залучення правоохоронних органів (потенційні – для ситуацій, які були врегульовані в межах підприємства, і фактичні – для ситуацій, за якими були залучені правоохоронні органи).

Формула розрахунку економічного ефекту на рівні підприємства від **скорочення витрат на реагування на ризики**:

$$EE_{rt} = \sum_{i=1}^{I}\left(C_{a,i} - C_i\right) + \left(S_a - S\right),$$

де EE_{le} – загальний економічний ефект від скорочення витрат на реагування на ризики;

S_a – витрати на функціонування альтернативної аналогічної системи (наприклад, залучення сторонніх постачальників послуг, упровадження альтернативних автоматизованих систем тощо);

$C_{a,i}$ – витрати на реагування на i-й ризик із використанням альтернативних (наприклад, уже реалізованих на підприємстві) способів.

Очевидно, що економічний ефект щодо конкретного ризику може бути отриманий тільки якщо $C_i < C_{a,i}$.

Для розрахунку економічного ефекту від підвищення рівня дотримання законодавства, поліпшення захисту інтелектуальної власності та запобігання простоям і перебоям у діяльності підприємства необхідно за кожним ризиком мати обчислення відповідних потенційних втрат при реалізації конкретного ризику.

2. Розрахунок очікуваного економічного ефекту.

Наведені розрахунки можуть використовуватися за наявності повних даних по підприємству, коли можна шляхом прямої калькуляції складати збитки, витрати, економію та ін. за кожним ризиком. Такі розрахунки найбільшою мірою застосовні за наявності повних даних за минулі періоди. Однак коли йдеться про очікуваний (планований) економічний ефект, прогнозування ефекту на майбутні періоди та порівняння кількох методів економічного форензіку (наприклад, традиційного та цифрового), необхідно перейти від точних цифр за кожною дією та ризиком до середніх значень та ймовірностей, що значно ускладнює розрахунки. Підхід до таких розрахунків наведено нижче.

Умовні позначення:

A – загальна кількість подій, що відбуваються на підприємстві за певний період;

P_T – імовірність того, що та чи інша дія міститиме ризик для економічної безпеки підприємства;

P_R – імовірність реалізації ризику, через яку не було вжито заходів щодо мінімізації;

L_A – середній обсяг фактичної максимальної шкоди за ризиком, що реалізувався (максимальна шкода реалізується за відсутності вживання заходів щодо ризику);

P_G – можливість отримання сигналу про те, що дія є ризиком (% «спрацьовування»);

P_D – імовірність правильності отриманого сигналу про ризик, тобто відсоток підтверджених ризиків від кількості отриманих сигналів про ризик (% правильного «спрацьовування»);

P_N – середній відсоток ризиків, для яких вжито заходів щодо мінімізації збитків;

P_M – середній відсоток ризиків, для яких вжиті заходи щодо мінімізації збитків виявилися успішними та дозволили мінімізувати ймовірність настання інциденту;

P_K – середній відсоток, на який зменшилася ймовірність реалізації ризику (настання інциденту) в результаті вживання заходів щодо мінімізації ризику;

C_D – середні витрати на аналіз однієї дії;

C_K – середні витрати на мінімізацію шкоди за одним ризиком.

Максимальна шкода за відсутності реагування на ризики та спроб компенсації збитків від інцидентів становитиме

$$L_{max} = A \cdot P_T \cdot P_R \cdot L_A .$$

Збитки щодо ризиків, для яких було вжито заходів щодо мінімізації, і такі заходи виявилися успішними:

$$L_{M,S} = A \cdot P_T \cdot P_G \cdot P_D \cdot P_N \cdot P_M \cdot P_R \cdot (100\% - P_K) \cdot L_A .$$

Збитки щодо ризиків, для яких було вжито заходів щодо мінімізації, але такі заходи не мали позитивного результату:

$$L_{M,F} = A \cdot P_T \cdot P_G \cdot P_D \cdot P_N \cdot (100\% - P_M) \cdot P_R \cdot L_A .$$

Збитки щодо ризиків, для яких не було вжито заходів щодо мінімізації:

$$L_{M,N} = A \cdot P_T \cdot P_G \cdot P_D \cdot (100\% - P_N) \cdot P_R \cdot L_A .$$

Витрати на аналіз дій щодо ризиків:

$$C_A = A \cdot C_D \ .$$

Витрати на мінімізацію виявлених ризиків:

$$C_M = A \cdot P_G \cdot C_K \ .$$

У такому випадку економічний ефект від мінімізації ризиків становитиме різницю між максимальними збитками від інцидентів за відсутності будь-якого реагування на ризики та збитками від інцидентів в умовах мінімізації ризиків (які, у свою чергу, складаються зі збитків від інцидентів за ризиками, для яких заходи реагування не вживалися (вживалися, але не були успішними; вживалися, але ризик все одно реалізувався) з урахуванням витрат на аналіз дій і мінімізацію ризиків:

$$EE_{dp}^{*} = L_{max} - L_{M,S} - L_{M,F} - L_{M,N} - C_A - C_M \ .$$

Отже, загальна кількість інцидентів з урахуванням заходів щодо мінімізації ризиків складається з інцидентів, пов'язаних із ризиками, які не вдалося виявити, реалізованих ризиків, за якими не було вжито заходів щодо мінімізації, та ризиків, за якими було вжито заходів, які в результаті не привели до зниження ймовірності інциденту, та розраховуватиметься в такий спосіб:

$$I = A \cdot P_T \cdot (100\% - P_G) \cdot P_R + \\ + A \cdot P_T \cdot P_G \cdot P_D \cdot (100\% - P_N) \cdot P_R + \\ + A \cdot P_T \cdot P_G \cdot P_D \cdot P_N \cdot (100\% - P_M) \cdot P_R \ .$$

Після настання інцидентів, які завдають економічних збитків, підприємство вживає заходів щодо компенсації збитків як самостійно, без звернення до правоохоронних органів (медіація між задіяними сторонами та спроба досягти добровільної компенсації шкоди винними особами), так і шляхом залучення правоохоронних органів з метою примусового відшкодування особами, винними в заподіянні шкоди.

Умовні позначення:

P_I – середній відсоток інцидентів, за якими було здійснено спробу врегулювання без звернення до правоохоронних органів;

$P_{I,S}$ – імовірність успішності спроб врегулювання інцидентів без звернення до правоохоронних органів;

C_I – середні витрати на розгляд одного інциденту без звернення до правоохоронних органів;

$P_{I,C}$ – середній відсоток компенсації збитків при врегулюванні інцидентів без звернення до правоохоронних органів;

$P_{L,S}$ – імовірність успішності спроб врегулювання інцидентів при зверненні до правоохоронних органів;

$P_{L,C}$ – середній відсоток компенсації збитків при врегулюванні інцидентів при зверненні до правоохоронних органів;

C_L – середні витрати на розгляд одного інциденту при зверненні до правоохоронних органів.

Отримана сума компенсацій (як без звернення до правоохоронних органів, так і в результаті їх залучення) становитиме

$$W = I \cdot L_A \cdot P_I \cdot P_{I,S} \cdot P_{I,C} - I \cdot (1 - P_I) \cdot C_I + I \cdot L_A \cdot (1 - P_I) \cdot P_{L,S} \cdot P_{L,C} - I \cdot (1 - P_I) \cdot C_L .$$

Економічний ефект від врегулювання інцидентів без залучення правоохоронних органів може бути розрахований як різниця між сумами компенсацій, отриманими при використанні схеми, що передбачає вирішення частини інцидентів без звернення до правоохоронних органів, та сумами компенсацій, які були б отримані при передачі всіх інцидентів на розгляд до правоохоронних органів (у тому числі відповідні витрати):

$$EE_{rt}^{*} = W - I \cdot L_A \cdot P_{L,S} \cdot P_{L,C} - I \cdot C_L .$$

У такому випадку загальний економічний ефект від мінімізації ризиків та врегулювання інцидентів без залучення правоохоронних органів становитиме $EE^{*} = EE_{dp}^{*} + EE_{rt}^{*}$.

Економічний ефект для держави від упровадження інституційного механізму економічного форензіку на підприємствах складається з прямого зниження витрат на реалізацію державою своїх функцій завдяки зменшенню кількості звернень підприємств до правоохоронних органів, фінансового впливу на економіку та бюджетну систему, поліпшення показників окремих підприємств, а також з опосередкованих системних ефектів економічного форензіку, таких як підвищення рівня дотримання законодавства у сфері інтелектуальної власності та обробки персональних даних, зниження рівня економічної злочинності та загальне поліпшення економічної ситуації.

Формула розрахунку економічного ефекту на рівні держави від **зниження навантаження на правоохоронні органи** передбачає визначення кількості звернень, яким вдалося запобігти, по всіх підприємствах і множення цієї кількості на середні витрати держави в розрахунку на одне звернення (заяву):

$$GE_{le} = P \sum_{j=1}^{J} \sum_{i=1}^{I_j} a_i \ ,$$

де GE_{le} – сума економічного ефекту для держави від зниження навантаження на правоохоронні органи;

P – середні витрати держави на весь цикл розгляду однієї заяви підприємства до правоохоронних органів, включаючи розгляд у всіх задіяних правоохоронних органах та судовій системі протягом усього періоду до закриття справи або припинення подання повторних заяв з боку підприємства;

J – загальна кількість підприємств, на яких запроваджено економічний форензік у рамках інституційного механізму;

I_j – загальна кількість ризиків, що підтвердилися, за певний період на j-му підприємстві;

a_i – оператор, що вказує на факт запобігання зверненню до правоохоронних органів, може набувати значення 0, якщо підприємству довелося звернутися до правоохоронних органів, або 1, якщо ситуація була врегульована в межах підприємства без необхідності їх залучення.

Формула розрахунку економічного ефекту на рівні держави загалом від **поліпшення економічних показників підприємств за рахунок зниження збитків:**

$$GE_{dp} = \sum_{j=1}^{J} \sum_{i=1}^{I_j} EE_{dp,j} \ ,$$

де GE_{dp} – сума економічного ефекту на рівні економіки загалом від поліпшення економічних показників підприємств;

$EE_{dp,j}$ – загальний економічний ефект від запобігання фінансовим збиткам у результаті здійснення економічного форензіку на j-му підприємстві.

Практичну апробацію запропонованих підходів до впровадження інструментів цифрового економічного форензіку виконано у ПрАТ «Український авіаційно-технічний центр» і ПНВК «Інтербізнес». Для ПрАТ «Український авіаційно-технічний центр» основним видом діяльності є «ремонт і технічне обслуговування повітряних і космічних літальних апаратів». ПНВК «Інтербізнес» переважно здійснює розведення свійської птиці.

До цього часу на зазначених підприємствах методи економічного форензіку системно не застосовувалися (ані традиційного, ані цифрового), а моніторинг ризиків зводився до стандартних епізо-

дичних процедур аудиту, контролю з боку відповідальних осіб (керівників структурних підрозділів). У результаті впроваджено методи й інструменти моніторингу дій на предмет загроз економічній безпеці (зокрема, завищених цін закупівель, списання втрачених активів та ін.) й активізовано розслідування конкретних ситуацій та їх врегулювання без залучення правоохоронних органів. Для оцінювання економічного ефекту на підприємствах проведено анкетування. Макет анкети, а також оцінені за допомогою анкетування зміни основних показників щодо виявлення інцидентів у сфері економічної безпеки та реагування на них у результаті впровадження цифрового економічного форензіку у ПрАТ «Український авіаційно-технічний центр» наведено в табл. 3.3.

Після впровадження системи цифрового економічного форензіку у ПрАТ «Український авіаційно-технічний центр» значно зросла кількість аналізованих дій, а також відповідні витрати. Це обґрунтовано тим, що до впровадження відповідного інструментарію такі витрати були мінімальними, але й охоплення дій аналізом було також мінімальним, що не дозволяло виявляти потенційні ризики у сфері економічної безпеки. У результаті використання інструментів аналізу дій кількість виявлених ризиків значно збільшилася, що привело до більш активного вживання заходів щодо їхньої мінімізації та сприяло зменшенню кількості фактичних інцидентів. Завдяки акценту на спроби внутрішнього врегулювання інцидентів знизилася потреба в залученні правоохоронних органів, а також скоротилися відповідні витрати. Водночас інтенсифікація процесів внутрішнього врегулювання дозволила значною мірою збільшити суми компенсацій за врегульованими інцидентами.

Аналогічні інструменти використано в приватній науково-виробничій компанії «Інтербізнес»: за рахунок упровадження системи аналізу потенційних ризиків, насамперед у сфері закупівель сировини за завищеними цінами, необґрунтованого списання втрат сировини, а також реалізації продукції за заниженими цінами, вдалося запобігти суттєвим фінансовим втратам (табл. 3.4).

Розрахунок економічного ефекту від упровадження системи цифрового економічного форензіку у ПрАТ «Український авіаційно-технічний центр» і ПНВК «Інтербізнес» з розбивкою на джерела ефекту та напрями витрат наведено в табл. 3.5.

Таблиця 3.3. **Анкета оцінки зміни основних показників підприємств після впровадження інструментів цифрового економічного форензіку та результати ПрАТ «Український авіаційно-технічний центр» у 2022-2023 рр.**

Показник	До впровадження (2022 р.)	Після впровадження (2023 р.)	Різниця, %
1	2	3	4
Загальні показники			
Чисельність співробітників, осіб	53	56	5,66
Виручка від реалізації, тис. грн	21 513	23 589	9,65
Операційні витрати, тис. грн	641	651	1,56
Собівартість реалізованої продукції, тис. грн	15 911	17 241	8,36
Прибуток (збиток), тис. грн	2 824	3 081	9,10
Показники, пов'язані із системою форензіку			
Загальна кількість дій	2486	2512	1,05
Кількість проаналізованих дій	256	2315	804,30
Загальні витрати на аналіз дій, тис. грн	15	127	746,67
Кількість виявлених ризиків у сфері економічної безпеки	22	56	154,55
Кількість ризиків, стосовно яких вжито заходів щодо мінімізації	14	37	164,29
Загальна кількість інцидентів у сфері економічної безпеки	12	6	-50,00
- із них за ризиками, виявленими у процесі аналізу дій	4	5	25,00
- за ризиками, стосовно яких вжито заходів щодо мінімізації	3	4	33,33
Загальні витрати на вживання заходів щодо мінімізації ризиків, тис. грн	76	225	196,05
Сумарні збитки за всіма інцидентами, тис. грн	2326	715	-69,26
Кількість інцидентів, за якими здійснено спробу внутрішнього врегулювання	3	5	66,67

Закінчення табл. 3.3

1	2	3	4
- із них кількість врегульованих	1	4	300,00
- загальна сума компенсації за врегульованими, тис. грн	313	417	33,23
- загальна сума витрат на спроби внутрішнього врегулювання, тис. грн	15	35	133,33
Кількість інцидентів, переданих до правоохоронних органів	3	1	-66,67
- із них після спроби внутрішнього врегулювання	2	1	-50,00
- кількість врегульованих	1	1	0,00
- загальна сума компенсації за врегульованими інцидентами, тис. грн	97	104	7,22
- сумарні витрати на розгляд у правоохоронних органах, тис. грн	82	21	-74,39

Джерело: складено автором.

Таблиця 3.4. **Оцінка зміни основних показників підприємств після впровадження інструментів цифрового економічного форензіку на птахофабриках[2] ПНВК «Інтербізнес» в 2022-2023 рр.**

Показник	До впровадження (2022 р.)	Після впровадження (2023 р.)	Різниця, %
1	2	3	4
Загальні показники			
Чисельність співробітників, осіб	502	500	-0,40
Виручка від реалізації, тис. грн	837 414,611	920 234,92	9,89
Операційні витрати, тис. грн	108 647, 408	123 466,91	13,64
Собівартість реалізованої продукції, тис. грн	682 823,247	669 439,91	-1,96
Прибуток (збиток), тис. грн	45 943,957	51 622,63	12,36

[2] У розрахунку використано дані з 4 птахофабрик: Богодухівськоої, Городищенської, Запорізької, Черкаської.

Закінчення табл. 3.4

1	2	3	4
Показники, пов'язані із системою форензіку			
Загальна кількість дій	32 724	31 513	-3,70
Кількість проаналізованих дій	3261	25755	689,79
Загальні витрати на аналіз дій, тис. грн	195	1436	636,41
Кількість виявлених ризиків у сфері економічної безпеки	450	5614	1 147,56
Кількість ризиків, стосовно яких вжито заходів щодо мінімізації	200	3800	1 800,00
Загальна кількість інцидентів у сфері економічної безпеки	357	294	-17,65
- із них за ризиками, виявленими у процесі аналізу дій	284	238	-16,20
- за ризиками, стосовно яких вжито заходів щодо мінімізації	215	221	2,79
Загальні витрати на вживання заходів щодо мінімізації ризиків, тис. грн	532	4051	661,47
Сумарні збитки за всіма інцидентами, тис. грн	37021	28770	-22,29
Кількість інцидентів, за якими здійснено спробу внутрішнього врегулювання	137	735	436,50
- із них кількість врегульованих	127	210	65,35
- загальна сума компенсації за врегульованими, тис. грн	7292	8324	14,15
- загальна сума витрат на спроби внутрішнього врегулювання, тис. грн	1325	3470	161,89
Кількість інцидентів, переданих до правоохоронних органів	19	23	21,05
- із них після спроби внутрішнього врегулювання	8	21	162,50
- кількість врегульованих	7	11	57,14
- загальна сума компенсації за врегульованими інцидентами, тис. грн	532	1274	139,47
- сумарні витрати на розгляд у правоохоронних органах, тис. грн	1271	739	-41,86

Джерело: складено автором.

Таблиця 3.5. **Розрахунок економічного ефекту від упровадження цифрового економічного форензіку на підприємствах ПрАТ «Український авіаційно-технічний центр» і ПНВК «Інтербізнес», тис. грн**

Витрати та джерела економічного ефекту	Сума економічного ефекту	
	ПрАТ «УАТЦ»	ПНВК «Інтербізнес»
Додаткові витрати		
Аналіз дій	-112	-1241
Вживання заходів щодо мінімізації ризиків	-149	-3519
Спроби внутрішнього врегулювання	-20	-598
Джерела економічного ефекту		
Зменшення збитків за інцидентами	1611	8251
Зменшення витрат на розгляд у правоохоронних органах	61	532
Збільшення суми компенсацій збитків у процесі внутрішнього врегулювання	104	1032
Загальний економічний ефект	1495	4457

Джерело: складено автором.

Отже, в обох випадках реалізації запропонованого підходу економічний ефект досягнуто за рахунок зменшення збитків за інцидентами, витрат на розгляд інцидентів у правоохоронних органах та збільшення суми компенсацій збитків у процесі внутрішнього врегулювання.

3.3 Стратегічні напрями впровадження інституційного механізму економічного форензіку на підприємствах України

Система економічного форензіку є ефективним інструментом виявлення та реагування на економічні ризики окремого підприємства, проте її інституційна реалізація в рамках цілісної державної стратегії дозволяє набути додаткових переваг на макрорівні. Наразі використання цифрового економічного форензіку на підприємствах безпосередньо не регламентовано, тому актуальними є пропозиції щодо державної політики у сфері створення та функціонування

запропонованого інституційного механізму економічного форензіку на підприємствах України.

Встановлено, що завдання, які покладаються на систему економічного форензіку на підприємствах, значною мірою збігаються із завданнями Бюро економічної безпеки України (БЕБ), а саме: збір та аналіз інформації про правопорушення, що впливають на економічну безпеку держави, визначення способів запобігання їх виникненню в майбутньому. Тому БЕБ доцільно вважати основним органом для координації державних заходів щодо застосування інструментів цифрового економічного форензіку на підприємствах. Крім того, з урахуванням сучасних тенденцій, пов'язаних з упровадженням у фінансову систему віртуальних активів (зокрема криптовалют), що супроводжується їх поширеним використанням з метою здійснення та приховування злочинів, у рамках форензіку на державному рівні необхідно в пріоритетному порядку розвинути функції контролю за такими активами та запобігання їх використанню в злочинній діяльності.

На рис. 3.5 наведено загальну схему організації економічного форензіку на державному рівні в рамках запропонованого інституційного механізму.

Як і на рівні підприємства, на рівні держави економічний форензік реалізується у вигляді низки процесів, що здійснюються певними організаційними елементами з використанням відповідного інструментарію.

Підтримка інформаційної інфраструктури. На державному рівні необхідно створити інформаційну інфраструктуру для централізованого збору, зберігання та обробки інформації із систем економічного форензіку окремих підприємств. Дану інформацію слід використовувати у формі автоматизованих робочих місць для конкретних фахівців, за якими будуть закріплені функції нагляду за впровадженням і функціонуванням системи економічного форензіку на підприємствах, а також за використанням її результатів в інтересах інших підприємств загалом. Стосовно державних підприємств ці функції потенційно можна покласти на БЕБ, оскільки економічна безпека державних підприємств є невід'ємною складовою економічної безпеки держави. Інформаційна інфраструктура має включати сервери, бази даних, інтерфейси обміну інформацією з підприємствами, інструменти автоматизованої обробки інформації, візуалізації та створення звітів (див. рис. 3.5).

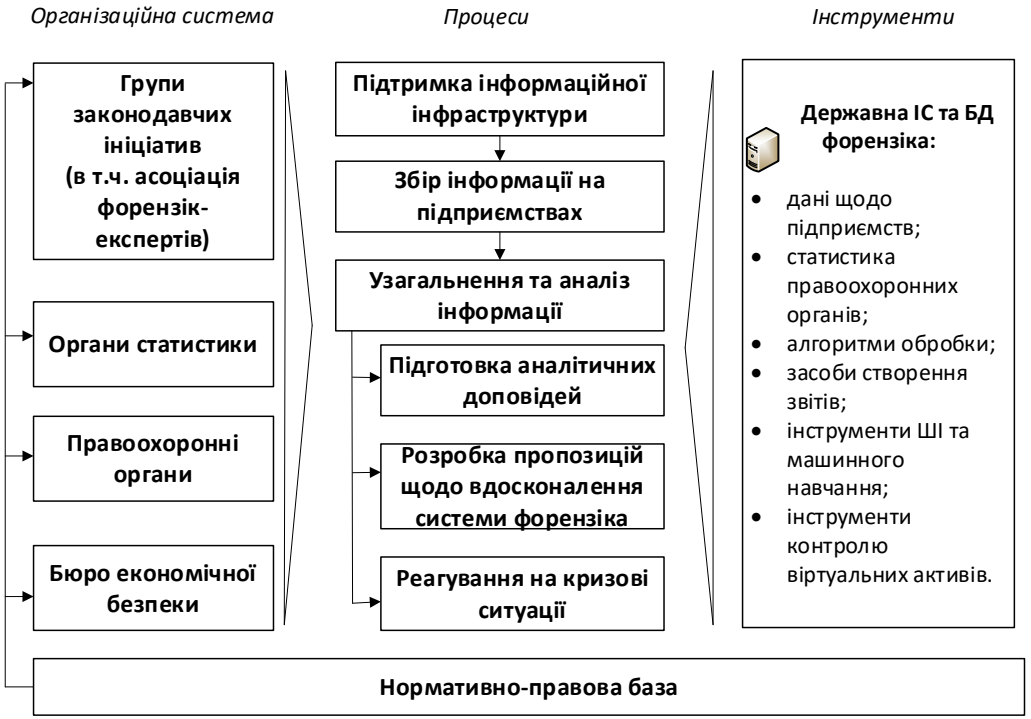

Рис. 3.5. **Елементи забезпечення інституційного механізму економічного форензіку на державному рівні**

Джерело: складено автором.

Збір інформації на підприємствах. Інформація, зібрана на окремих підприємствах, надходить у єдину державну інформаційну систему. Залежно від особливостей регулювання конфіденційності вона може як знеособлюватися, так і бути доступною для конкретного підприємства. З метою забезпечення повноти інформації, що надходить від підприємств, її надання слід регламентувати на законодавчому рівні, а не здійснювати за бажанням. Інформація може надаватися як у процесі поступового заповнення баз даних на підприємствах, так і з певною періодичністю (наприклад, раз на квартал). Зібрана інформація зберігається в централізованій базі для подальшого використання.

Узагальнення й аналіз інформації. Зібрана інформація узагальнюється (розраховуються сумарні, середні, питомі та ін. значення) з метою подальшого аналізу. Зокрема, для аналітичних цілей на державному рівні можуть бути корисними такі показники:

кількість і відсоток (від загальної кількості операцій за категоріями) операцій, що містять ризики для економічної безпеки підприємства;

потенційні та фактичні збитки від виявлених ризиків;

відсоток правильної класифікації ситуацій (віднесення до ризиків);

середній час врегулювання в межах підприємства;

відсоток ситуацій, врегульованих у межах підприємства порівняно до відсотка ситуацій, за якими доводиться звертатися до правоохоронних органів;

загальні та питомі витрати на запобігання ризикам і усунення наслідків інцидентів;

економічний ефект заходів, спрямованих на запобігання ризикам (як різниця між потенційними збитками та сумою фактичної шкоди й витрат на мінімізацію ризиків і усунення їх наслідків) у розрізі врегулювання в межах підприємства та залучення правоохоронних органів;

середній час, що витрачається на врегулювання проблемних ситуацій (як у межах підприємства, так і із залученням правоохоронних органів).

Усі ці показники можуть аналізуватися за галузями, формами власності тощо. Крім перелічених, можна запропонувати багато інших окремих, зведених і відносних показників. Використання

комплексу показників дозволить отримати повне уявлення про ефективність економічного форензіку в масштабі країни. Для аналізу даних і виявлення тенденцій доцільно використовувати засоби штучного інтелекту та машинного навчання.

Також окремим елементом є аналіз показників використання віртуальних активів.

За результатами аналізу інформації державні органи можуть **готувати аналітичні доповіді**, що містять зведені показники за результатами застосування інструментарію економічного форензіку за звітний період, основні висновки та рекомендації щодо вдосконалення системи економічного форензіку (як для підприємств, так і для органів державної влади), статистичну інформацію для включення до збірників тощо.

Також можуть **розроблятися пропозиції щодо внесення змін до законодавства**, яке регулює економічний форензік на підприємствах. Це можуть бути пропозиції як щодо організації системи економічного форензіку безпосередньо на підприємствах (перелік інформації, що збирається, відстежувані показники, порядок розгляду спорів, процедури медіації, способи повідомлення державних органів), так і щодо використання її результатів органами державної влади для прийняття рішень (удосконалення правозастосовної практики при розгляді спорів суб'єктів господарювання зі співробітниками або контрагентами, що виникають унаслідок реалізації ризиків та настання інцидентів, виявлених при реалізації процедур форензіку тощо).

Крім того, в інституційний механізм закладена можливість **реагування на кризові ситуації**, такі як різке підвищення кількості ризиків певного типу, виникнення нових ризиків, зростання обсягу втрат від ризиків, ненадання інформації великою кількістю підприємств, приховування чи викривлення даних. Для кожної типової кризової ситуації мають бути розроблені критерії визначення (наприклад, граничні значення показників), процедури реагування та притягнення до відповідальності винних осіб (якщо з'ясується зловмисний характер виникнення ситуації).

Ключовим елементом інституційного механізму економічного форензіку на державному рівні є інформаційні системи та бази даних, які забезпечують безперебійне функціонування інформаційної інфраструктури економічного форензіку. Таку інфраструктуру

доцільно реалізувати у вигляді бази даних, де консолідується інформація з окремих підприємств, та єдиної державної інформаційної системи, що забезпечує введення, аналіз та виведення інформації у зручному для користувача форматі (форми введення інформації, інформаційні панелі, автоматичне створення звітів, сигнали про виникнення кризових ситуацій). Для обробки інформації можуть також застосовуватися інструменти машинного навчання, ШІ та блокчейну, які завдяки наявності великих інформаційних масивів, зібраних на основі інформації з великої кількості підприємств, працюватимуть набагато ефективніше порівняно з їх застосуванням виключно на основі даних одного підприємства.

З організаційної точки зору впровадження економічного форензіку потребує залучення БЕБ (передусім відносно державних підприємств цей орган має потенціал стати базовим для реалізації системи економічного форензіку) у координації з Кабінетом Міністрів України, органів статистики як джерела інформації та одержувача зібраних системою економічного форензіку даних, правоохоронних органів для вживання заходів у разі виявлення порушень й удосконалення правозастосовної практики, а також груп законодавчих ініціатив для законодавчого регламентування практики економічного форензіку та розроблення змін до законодавства за результатами аналізу отриманих у процесі економічного форензіку даних (наприклад, удосконалення законодавства з питань вирішення господарських спорів чи господарської діяльності загалом).

Переваги впровадження такого механізму на державному рівні полягають у такому:

підвищення обізнаності органів влади про економічні ризики та загрози, характерні для підприємств, у тому числі можливості класифікації за масштабом підприємств, галузями, формами власності тощо;

забезпечення «наскрізної видимості» ситуації з економічним форензіком на підприємствах, створення «моментальної фотографії» ситуації у певні моменти часу;

можливість оцінювання ділової репутації конкретних власників і співробітників підприємств (наприклад, коли у власників виникають проблеми, що повторюються, на різних підприємствах або після зміни власності);

можливість відстежувати вплив управлінських рішень на основні показники системи економічного форензіку при реалізації заходів щодо вдосконалення системи;

оцінювання збитків від певних дій, а також економічного ефекту від економічного форензіку в масштабах економіки країни.

На практиці реалізація викладених положень інституційного механізму відбувається шляхом здійснення організаційних і законодавчих ініціатив, що сприяють як упровадженню інструментарію форензіку на підприємствах, так і виконанню державою регулюючих, координуючих та стимулюючих заходів у цій сфері. Основні сфери таких ініціатив включають:

1. Формування законодавчих засад.

Основним способом реалізації державою політики у сфері впровадження та використання інструментів цифрового економічного форензіку на підприємствах є формування законодавчих засад для цього. Слід ураховувати, що залученість держави має бути мінімальною, оскільки одним з основних принципів економічного форензіку є орієнтація на максимальне врегулювання кризових ситуацій у межах підприємства без залучення держави, а саме правоохоронних органів.

Законодавчі ініціативи можуть бути спрямовані, зокрема, на такі сфери застосування механізму економічного форензіку:

створення законодавчих умов для врегулювання інцидентів силами підприємств без звернення до правоохоронних органів, наприклад, у сфері наділення юридичною силою рішень органів медіації на підприємствах, регламентації застосування штрафних санкцій щодо працівників (щоб уникнути конфліктів із трудовим законодавством) або контрагентів, визначення порядку отримання компенсацій від осіб, винних в інцидентах;

створення умов, що стимулюють до врегулювання інцидентів без залучення правоохоронних органів, наприклад шляхом надання засобів державної підтримки за певних показників внутрішнього врегулювання інцидентів і спорів, а також надання юридичної сили взаємним зобов'язанням сторін, прийнятим під час врегулювання інцидентів (щоб уникнути дублювання процесів задля забезпечення можливостей примусового виконання);

регламентація обов'язків підприємств надавати державі інформацію про інциденти та їх врегулювання, зокрема шляхом внесення відповідних відомостей до державної інформаційної системи безпосередньо або до корпоративної системи з автоматичною передачею інформації до державної інформаційної системи.

2. Створення інформаційної інфраструктури.

Щоб максимально використати можливості стимулювання впровадження інструментів цифрового економічного форензіку, державі необхідно розгорнути відповідну інформаційну інфраструктуру, яка охоплює інформаційну систему для збору, обробки та аналізу інформації від підприємств, робочі місця фахівців, систему повідомлення та реагування на кризові ситуації, систему передачі інформації до статистичних органів для подальшого узагальнення та публікації.

Також доцільною є підтримка на рівні держави розроблення типової мінімально необхідної (базової) системи цифрового економічного форензіку для підприємств, які не мають можливості розробити власну систему або придбати готове комерційне рішення. Уже сама доступність цієї системи стимулюватиме підприємства до випробування такого інструментарію.

Крім того, держава може надавати підприємствам за передплатою або розміщувати у відкритому доступі такі інформаційні продукти, як «білі» та «чорні» списки (благонадійних і неблагонадійних підприємств та посадових осіб відповідно), навчальні матеріали з користування інформаційними системами, з цифрового економічного форензіку в цілому, а також за окремими сферами, у яких часто виникають загрози економічній безпеці, зокрема «відмивання» злочинних доходів, недотримання законодавства, зловживання під час закупівлі, охорона прав інтелектуальної власності, захист персональних даних тощо.

3. Регулювання.

За наявності дієвої системи реалізації державної політики у сфері цифрового економічного форензіку (зокрема законодавчих основ та інформаційної інфраструктури) держава може виконувати певні регулюючі функції з метою підвищення ефективності використання інструментарію цифрового економічного форензіку, збільшення охоплення підприємств, забезпечення отримання відпові-

дальними державними органами інформації від підприємств, а також релевантне реагування на кризові ситуації. При цьому регулювання повинне мати м'який характер, оскільки внутрішньокорпоративний цифровий економічний форензік націлений, насамперед, на запобігання інцидентам та їх врегулювання власними силами підприємств із мінімальним залученням держави загалом та правоохоронних органів зокрема.

Державні заходи регулювання можуть вживатися, зокрема, в таких ситуаціях:

різке погіршення основних показників (зменшення відсотка інцидентів, врегульованих без залучення правоохоронних органів, зниження обсягу компенсованих збитків, різке зростання кількості звернень до правоохоронних органів);

зниження кількості підприємств, які надають звітність про функціонування інструментів електронного економічного форензіку – для перевірки роботи інформаційних систем і стимулювання підприємств до подання звітності;

надходження від підприємств скарг на державну політику у сфері економічного форензіку (зокрема на її законодавче забезпечення) чи роботу інформаційних систем (або інші технічні аспекти).

4. Стимулювання.

Заходи державного стимулювання запровадження інструментів цифрового економічного форензіку можуть включати:

безкоштовне надання відповідних інформаційних систем (або доступу до вебінтерфейсу хмарного рішення) та іншого програмного забезпечення й інформаційної інфраструктури;

нефінансові пільги для підприємств, які демонструють високі стандарти у сфері дотримання законодавства (низька кількість економічних злочинів, порушень інтелектуальної власності та захисту персональних даних тощо), наприклад шляхом внесення до реєстру підприємств із високим рівнем економічної безпеки.

5. Координація.

Держава може координувати впровадження на підприємствах інформаційних систем, що реалізують інструменти цифрового економічного форензіку, організовувати обмін досвідом як між підприємствами (горизонтальні зв'язки), так і між державними або місцевими органами влади та підприємствами (вертикальні зв'язки).

Також доцільним є обмін досвідом між окремими органами державної влади, які відповідають за питання впровадження цифрового економічного форензіку. У разі виникнення кризових ситуацій держава може координувати реалізацію заходів реагування із залученням державних органів та окремих підприємств. Крім того, координація є обґрунтованою при внесенні змін до законодавства, інформаційних систем чи інших аспектів практики цифрового економічного форензіку – для якнайшвидшого та максимально безпроблемного впровадження таких змін.

Функції окремих органів державної влади у впровадженні та реалізації інституційного механізму економічного форензіку на підприємствах полягають у такому.

Бюро економічної безпеки:

готує пропозиції щодо нормативного регулювання функціонування системи цифрового економічного форензіку на державних підприємствах (регламентація порядку застосування інструментів, використання інформаційних систем, а також прав та обов'язків підприємств) – рішення можуть оформлюватися як у форматі наказів БЕБ, так і у вигляді постанов Кабінету Міністрів;

складає технічне завдання на розроблення типової системи (або модуля) цифрового економічного форензіку, яка поширюватиметься безкоштовно серед підприємств, які не вважають за доцільне або не мають можливості розробити власні або купити готові рішення або прагнуть здійснити тестове використання таких рішень;

складає технічне завдання на розроблення державної інформаційної системи для збору та аналізу інформації про функціонування інструментів цифрового економічного форензіку від підприємств, а також для підтримки ухвалення відповідних управлінських рішень;

організує підтримку інформаційної інфраструктури (насамперед державну інформаційну систему та відповідні бази даних, а також канали обміну інформацією з підприємствами);

складає списки показників, які підприємства мають надавати державі через інформаційну систему, а також розрахункові показники, що використовуються в аналітичних цілях;

публікує звіти про роботу системи цифрового економічного форензіку на підприємствах, зокрема про охоплення підприємств використанням відповідних інструментів і практик, показники еко-

номічного ефекту від застосування цифрового економічного форензіку (як сумарно по підприємствах, так і на рівні держави загалом), а передусім про рівень запобігання збиткам, обсяг отриманих компенсацій та економії за рахунок врегулювання інцидентів без залучення правоохоронних органів;

розробляє заходи щодо стимулювання підприємств до впровадження цифрового економічного форензіку, вчасного та повного надання інформації державним органам, врегулювання інцидентів без залучення правоохоронних органів;

складає (на основі різних вітчизняних і зарубіжних джерел, у тому числі даних із систем форензіку, аналізу відкритих джерел та бази судових рішень) і публікує «білий» та «чорний» списки підприємств, а також осіб з точки зору їх надійності як потенційних контрагентів чи співробітників;

оцінює вплив використання інструментів цифрового економічного форензіку на економіку з урахуванням показників господарської діяльності підприємств, бази оподаткування та податкових надходжень, інвестиційного клімату, економічних злочинів і правопорушень, взаємодії із зарубіжними контрагентами тощо;

здійснює моніторинг обігу цифрових віртуальних активів, тобто активів на базі сучасних цифрових технологій (блокчейну та смарт-контрактів), а також можливих випадків зловживання та шахрайства, відстеження проникнення таких активів у фінансову систему тощо.

Правоохоронні органи:

розглядають та приймають рішення щодо інцидентів, які підприємствам не вдалося вирішити власними силами або за взаємною згодою сторін (підприємства, їх співробітники та контрагенти);

за необхідності забезпечують примус до виконання рішень, прийнятих під час врегулювання інцидентів у межах підприємства (переважно стягнення збитків, анулювання документів, виконання чи відмова від тих чи інших дій);

здійснюють статистичний облік правопорушень, що охоплює цифровий економічний форензік і використовується як для вдосконалення розгляду таких правопорушень, так і для порівняння з показниками, про які звітують самі підприємства;

формують пропозиції щодо вдосконалення законодавства та правозастосовної практики, спрямовані на мінімізацію кількості

звернень підприємств до правоохоронних органів і переважне врегулювання інцидентів власними силами підприємств;

сприяють БЕБ у складанні «білих» і «чорних» списків підприємств, а також осіб з позиції їхньої благонадійності як потенційних контрагентів чи посадових осіб;

оцінюють економічний ефект для правоохоронних органів, досягнутий за рахунок врегулювання підприємствами інцидентів без залучення правоохоронних органів.

Судова система (судові органи):

приймає висновки від форензік-експертів для використання в розгляді справ;

запрошує форензік-експертів до розгляду справ.

Органи статистики:

збирають і публікують статистичні дані, пов'язані з функціонуванням системи цифрового економічного форензіку, зокрема, про кількість виявлених або попереджених інцидентів, компенсовані втрати, відносні показники (відсоток кількості інцидентів, врегульованих власними силами підприємства, порівняно з кількістю звернень до правоохоронних органів, відсоток попереджених інцидентів, обсяг компенсованих втрат та ін.);

надають статистичну інформацію зацікавленим сторонам, у тому числі БЕБ, Кабінету Міністрів, зокрема Міністерству економіки, конкретним підприємствам та їх об'єднанням.

Групи законодавчих ініціатив:

аналізують нормативно-правові акти та формують для органів влади пропозиції щодо вдосконалення державного регулювання й нормативних аспектів цифрового економічного форензіку. Ці групи можуть формуватися з представників підприємств, їх об'єднань (асоціацій), галузевих організацій, торгово-промислових палат та інших зацікавлених осіб. До груп законодавчих ініціатив можуть входити як представники підприємств та їх асоціацій, так і депутати всіх рівнів;

засновують самоврядні організації для консолідації діяльності форензік-спільноти, здійснюють сертифікацію діяльності своїх членів.

На рис. 3.6 відображено взаємозв’язок між зацікавленими сторонами та їхню взаємодію в процесі функціонування системи цифрового економічного форензіку на підприємствах.

Рис. 3.6. **Взаємозв'язок і взаємодія між зацікавленими сторонами в процесі функціонування системи економічного форензіку на підприємствах**

Джерело: складено автором.

Таким чином, інституційний механізм економічного форензіку на підприємствах України сформульовано на рівні рекомендацій для органів державної влади щодо формування законодавчих засад, створення інформаційної інфраструктури, регулювання, стимулювання та координації процесів упровадження економічного форензіку. Виокремлено ключові функції основних зацікавлених осіб, у тому числі БЕБ, правоохоронних органів, органів статистики та груп законодавчих ініціатив, спрямовані на прискорення впровадження цифрового економічного форензіку на підприємствах, підвищення ефективності прийняття державних рішень у сфері форензіку, зниження навантаження на правоохоронні органи, запобігання кризовим ситуаціям.

Висновки до розділу 3

1. Обґрунтовано необхідність реалізації економічного форензіку на підприємствах у формі єдиного інституційного механізму, орієнтованого на забезпечення економічної безпеки підприємств та держави як системи, що поєднує внутрішній взаємозв'язок і порядок здійснення процесів та процедур, а також їх методичне, організаційне, інформаційне, правове і ресурсне забезпечення та функціонування якої спрямоване на підвищення рівня економічної безпеки підприємств і держави на основі використання інструментів економічного форензіку. Такий механізм доцільно реалізувати на двох взаємозалежних рівнях – підприємств і держави.

2. Встановлено, що складові процеси інституційного механізму економічного форензіку на рівні підприємства включають збір та аналіз інформації, виявлення ризиків та підозрілих дій, реагування в межах підприємства з подальшим контролем за виконанням відповідних заходів і залученням правоохоронних органів. На рівні держави механізм передбачає підтримку інформаційної інфраструктури, збір інформації по підприємствах, а також узагальнення й аналіз даних, на основі яких складаються аналітичні доповіді, розробляються пропозиції щодо внесення змін до законодавства та здійснюється реагування на кризові ситуації.

3. Для забезпечення функціонування інституційного механізму економічного форензіку запропоновано створення інформацій-

ної інфраструктури, що включає інформаційну систему, бази даних та інструменти обробки даних із використанням машинного навчання та штучного інтелекту. Результатом упровадження механізму стане забезпечення систематизованого збору та аналізу інформації про господарські операції, пов'язані з потенційними ризиками для економічної безпеки підприємства, та реагування на такі ризики переважно в межах підприємства без залучення правоохоронних органів, забезпечення зручного доступу до інформації для прийняття державних рішень у цій сфері, у тому числі вдосконалення нормативного середовища економічного форензіку, а також зниження навантаження на правоохоронні органи за рахунок врегулювання проблемних ситуацій у межах підприємства.

4. За результатами аналізу потенційних джерел економічного ефекту застосування інструментів економічного форензіку на рівні окремого підприємства (запобігання фінансовим збиткам і витратам, пов'язаним із залученням правоохоронних органів, дотримання законодавства, захист інтелектуальної власності, скорочення витрат на реагування на ризики, поліпшення репутації тощо) та держави загалом (зниження навантаження на правоохоронні органи, поліпшення економічних показників підприємств за рахунок зниження обсягу шкоди і, відповідно, збільшення обсягу податкових надходжень, скорочення кількості інцидентів у сфері інтелектуальної власності та обробки персональних даних тощо) розроблено каузальну схему взаємозв'язку між ними та запропоновано методичний підхід до розрахунку економічного ефекту, досягнутого в результаті застосування економічного форензіку.

5. Здійснено апробацію запропонованого інституційного механізму економічного форензіку та верифікацію формул і показників на підприємствах ПрАТ «Український авіаційно-технічний центр» (економічний ефект становить 1 млн 495 тис. грн.) і ПНВК «Інтербізнес» (економічний ефект становить 4 млн 457 тис. грн). Обґрунтовано, що врахування ймовірностей правильної ідентифікації, мінімізації або усунення ризиків дозволяє підвищити точність оцінки фактичного та потенційного економічного ефекту, досягнутого в результаті застосування інструментів економічного форензіку.

6. Доведено, що системне впровадження інструментів економічного форензіку на підприємствах, а також реалізація відповід-

ного інституційного механізму на рівні держави здатні забезпечити економічний ефект не лише на рівні окремого підприємства, але і на рівні держави, а саме: зниження навантаження на систему правоохоронних органів, поліпшення економічних показників підприємств, збільшення обсягу податкових надходжень за рахунок зменшення збитків для підприємств, скорочення кількості інцидентів у сфері інтелектуальної власності та обробки персональних даних, зниження рівня економічної злочинності, загальне поліпшення економічної ситуації.

7. Розроблено стратегічні напрями імплементації інституційного механізму економічного форензіку на підприємствах України: формування законодавчих засад використання інструментів економічного форензіку; створення інформаційної інфраструктури; розроблення державних заходів; регулювання, стимулювання та координація застосування інструментів цифрового економічного форензіку. Визначено функціональну роль окремих органів державної влади у впровадженні та реалізації інституційного механізму економічного форензіку на підприємствах (Бюро економічної безпеки, правоохоронні органи, судова система, органи статистики, групи законодавчих ініціатив).

ВИСНОВКИ

Стрімкий розвиток цифрових технологій обумовлює зростання економічної злочинності, що потребує відповідного підвищення рівня економічної безпеки, а також активізації діяльності щодо розслідування таких злочинів, вчинених у тому числі через мережу Інтернет чи інші засоби цифрової комунікації. Тому надзвичайно актуальним є питання про поєднання традиційних, сучасних і перспективних організаційно-технологічних заходів й інструментів підвищення рівня економічної безпеки, серед яких класичний та цифровий форензік, для попередження ризиків та уникнення загроз скоєння економічних злочинів на підприємствах. Також форензік є інструментом антикорупційної профілактики, що вкрай важливо на шляху євроінтеграції як України загалом, так і окремих підприємств. Ефективна система економічного форензіку підвищує імовірність притягнення до відповідальності за економічні злочини, зміцнює усвідомлення неминучості наслідків і формує профілактичний ефект, що сприяє зменшенню кількості таких правопорушень у майбутньому.

Запропоновано вирішення актуального наукового завдання щодо використання економічного форензіку як безпекової інновації підприємства в умовах цифровізації економіки, що базується на таких висновках і положеннях.

1. На основі узагальнення уявлень науковців про сутність і визначення поняття «економічна безпека підприємства» виокремлено дві основні характерні ознаки терміна – стан і процес, що формує відповідно два підходи: системний (характерні риси, властивості системи, спроможність підприємства протидіяти загрозам і ризикам) та комплексний (комплекс заходів, що забезпечують стійке функціонування підприємства, економічну незалежність та протидію можливим загрозам та ризикам). Із використанням цих підходів економічний форензік визначено як складову комплексу заходів щодо *підтримки* стійкого функціонування та *протидії* економічним загрозам і ризикам.

2. Складність розгляду категорії економічного форензіку обумовлена такими аспектами: економічний форензік є безпековою інновацією, яка формується на перетині двох галузей науки – економіки та права; брак концептуальних досліджень щодо економічного форензіку пов’язаний з тим, що форензік передбачає використання методів й інструментів економіки для прийняття правових рішень, що формує прикладний характер його досліджень. Детальний роз-

гляд економічного форензіку як наукової дисципліни дозволяє стверджувати, що він генерує знання про досліджуваний предмет, існуючі та нові методи, підвищуючи доказову цінність економічного аналізу.

3. Встановлено, що в контексті даної роботи найбільш прийнятним є визначення терміна «економічний форензік» як дослідження передумов і наявності економічних злочинів на підприємствах з використанням методів й інструментів економічного аналізу (економіка) і фінансових розслідувань (право) з метою одержання інформації про встановлення фактів та обставин економічних злочинів для прийняття управлінських рішень й удосконалення стану економічної безпеки на підприємстві. У запропонованому трактуванні, на відміну від інших, сконцентровано особливості категорії (економіка – право), процесів (дослідження – одержання інформації) економічного форензіку та досягнення мети (посилення економічної безпеки підприємства). Сформульовано об'єкт дослідження економічного форензіку – економічні злочини на підприємствах і поведінка економічних злочинців, а також предмет – закономірності дослідження об'єктів на основі спеціальних пізнань, трансформованих у систему методів, інструментів і засобів вирішення питань щодо виявлення економічних злочинів.

4. Обґрунтовано актуальність упровадження в систему економічної безпеки підприємств процедури цифрового форензіку як відповіді на виклики цифровізації економіки та загрози, пов'язані з використанням цифрових технологій у протиправній діяльності. На основі узагальнення підходів до організації та реалізації цифрового форензіку запропоновано базову схему його здійснення для підприємств України та розроблено головні принципи для підвищення ефективності відповідних процедур. Суттєвою перевагою базової схеми порівняно з існуючими є те, що вона містить вичерпну та концентровану, проте не обтяжливу для реалізації інформацію про основні етапи здійснення цифрового форензіку.

5. Аналіз економічної злочинності у світі та Україні свідчить, що найбільш поширеними видами шахрайства є привласнення активів і корупція, а значних втрат підприємства зазнають унаслідок шахрайства з фінансовою звітністю. Більш вагомі загрози спостерігаються з боку зовнішнього середовища. Проте збільшення кількості випадків економічного шахрайства не впливає на активізацію моніторингу й аналізу діяльності. У результаті секторального порівняння застосування аналітики даних для боротьби з шахрайством встановлено, що в секторах «державні служби», «промислове виро-

бництво» та «фінансові послуги» має місце низький рівень використання аналізу даних, а отже, зберігається значний потенціал для поліпшення ситуації через більш технологічне опрацювання даних.

6. Встановлено, що однією з причин корпоративного шахрайства в Україні є зниження фінансових можливостей підприємств для забезпечення економічної безпеки, які відбуваються на тлі складних умов ведення бізнесу, пов'язаних із воєнним станом (що посилюють невизначеність і послаблюють «імунітет» підприємств до протиправних дій шахрайського характеру), та подальшого проникнення цифрових технологій, які створюють нові можливості для економічних шахраїв.

7. Визначено, що зовнішній аудит є найбільш ефективним інструментом для виявлення економічного шахрайства, але він, як й інші види контролю (внутрішній аудит, раптові перевірки, перевірки діяльності керівництва), не в змозі повернути втрачені кошти та відшкодувати збитки. Чинні інструменти протидії економічним злочинам мають обмежену ефективність, тому постає необхідність або їх удосконалення, або розширення наявного переліку.

8. На основі дослідження сучасної системи економічного форензіку окреслено практичну сферу його застосування, сформовано перелік основних послуг, пов'язаних з економічним форензіком, і розглянуто його методи, підходи та етапи. За результатами послідовного застосування аналізу та синтезу вдосконалено визначення суб'єкта та об'єкта проведення форензік-аудиту, а також уточнено перелік користувачів та очікуваний результат форензіку.

9. Розроблено концептуальні положення інституційного механізму економічного форензіку в Україні. Визначено, що складовими процесу на рівні підприємства є збір та аналіз інформації, виявлення ризиків і підозрілих дій, реагування в межах підприємства з подальшим контролем за виконанням і залученням правоохоронних органів; на рівні держави – підтримка інформаційної інфраструктури, збір статистичної інформації від підприємств, її узагальнення й аналіз, за результатами якого готуються аналітичні доповіді, розробляються пропозиції щодо внесення змін до законодавства. Для забезпечення функціонування механізму запропоновано створення інформаційної інфраструктури, що включає інформаційну систему, бази даних й інструменти обробки даних із використанням машинного навчання та штучного інтелекту.

10. Розроблено схеми застосування економічного форензіку на підприємствах і на державному рівні у рамках інституційного

механізму, складовими яких є організаційна система, процеси та інструменти економічного форензіку; наведено зміст кожного етапу економічного форензіку та функції учасників (оргсистеми). Також обґрунтовано використання інструментарію економічного форензіку підприємством з позиції супроводу конкретних процесів за допомогою програмних засобів і цифрових технологій.

11. Визначено основні переваги реалізації економічного форензіку для підприємств (мінімізація фінансових збитків і витрат, пов'язаних із залученням правоохоронних органів, захист інтелектуальної власності, скорочення витрат на реагування на ризики, запобігання простоям і перебоям у діяльності та ін.) і для держави (зниження навантаження на систему правоохоронних органів, поліпшення економічних показників підприємств через обмеження шкоди, збільшення обсягу податкових надходжень за рахунок зменшення збитків для підприємств, зниження рівня економічної злочинності та ін.).

12. Розроблено загальну каузальну схему одержання економічного ефекту від реалізації економічного форензіку, у тому числі встановлено джерела економічного ефекту на рівні окремого підприємства та держави загалом. Запропоновано інструментарій (аналітичні показники та формули розрахунків) і виконано оцінку ефекту економічного форензіку за перевагами, для яких можливим є прямий розрахунок. Обґрунтований інституційний механізм економічного форензіку апробовано та верифіковано шляхом розрахунку економічного ефекту від здійснення форензіку на підприємствах ПрАТ «Український авіаційно-технічний центр» (економічний ефект становить 1 млн 495 тис. грн) і ПНВК «Інтербізнес» (економічний ефект становить 4 млн 457 тис. грн).

13. Встановлено, що системне впровадження інструментів економічного форензіку на мікрорівні може принести економічний ефект як для підприємства, так і для держави. З метою просування та поширення використання економічного форензіку в Україні запропоновано стратегічні напрями впровадження на вітчизняних підприємствах інституційного механізму економічного форензіку для забезпечення економічної безпеки підприємств зокрема та держави загалом, а також визначено функціональну роль окремих органів державної влади у впровадженні та реалізації цього механізму.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бакай, В. Й. (2020). Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету, 4*(1), 32–35. https://doi.org/10.31891/2307-5740-2020-284-4-5

2. Барташевська, Ю. М. (2016). Економічна безпека підприємства: фактори впливу та шляхи забезпечення. *Економіка і суспільство, 7*, 189–194.

3. Бондар, Ю. А., & Дорошенко, Т. М. (2022). Економічна безпека підприємства як фактор забезпечення ефективності зовнішньоекономічної діяльності. В *Розвиток методів управління та господарювання на транспорті: Збірник наукових праць, 1*(78), 70–82. https://doi.org/10.31375/2226-1915-2022-1-70-82

4. Брюховецька, Н. Ю., Булєєв, І. П., & Чорна, О. А. (2024). Еволюція в підходах до управління підприємствами в умовах цифрових трансформацій. *Бізнес Інформ, 10*, 451–461. https://doi.org/10.32983/2222-4459-2024-10-451-461

5. Бюро економічної безпеки. (2024). *Звіт про діяльність БЕБ за 2023 рік*. https://esbu.gov.ua/storage/app/sites/32/2023%20рік/Звіт%20про%20діяльність%20БЕБ%20за%202023%20рік.pdf

6. Варналій, З., Буркальцева, Д., & Саєнко, О. (2011). *Економічна безпека України: проблеми та пріоритети зміцнення*. Київ: Знання України, 299 с.

7. Гапак, Н. М. (2013). Економічна безпека підприємства: сутність, зміст та основи оцінки. *Науковий вісник Ужгородського університету. Серія: Економіка, 3*(40), 62–65.

8. Геєць, В. М., Кизим, М. О., Клебанова, Т. С., & Черняк, О. І. (Ред.). (2006). *Моделювання економічної безпеки: держава, регіон, підприємство*. Харків: ІНЖЕК, 240 с.

9. Грибіненко, О. М., & Шагоян, С. М. (2017). Сутність та шляхи забезпечення економічної безпеки підприємства. *Науковий вісник Херсонського державного університету, 22*(1), 98–100.

10. Дасюк, В. (2024). Внутрішнє корпоративне шахрайство: які злочини найбільш розповсюджені. *Юридична газета*. https://yur-gazeta.com/publications/practice/kriminalne-pravo-ta-proces/vnutrishne-korporativne-shahraystvo-yaki-zlochini-naybilsh-rozpovsyudzheni.html

11. Державна служба статистики України. (2024). Фінансові результати до оподаткування підприємств за 2010-2024 роки. https://www.ukrstat.gov.ua/operativ/menu/menu_u/sze_20.htm

12. Державна служба статистики України. (2024a). Показники діяльності підприємств, згруповані за спеціальними агрегаціями, передбаченими у Регламенті (ЄС) 2020/1197 від 30.07.2020 щодо європейської статистики підприємств у 2010-2022 роках. https://www.ukrstat.gov.ua/operativ/menu/menu_u/sze_20.htm

13. Державна служба статистики України. (2024b). Капітальні інвестиції підприємств за видами економічної діяльності у 2012-2022 роках. https://www.ukrstat.gov.ua/operativ/menu/menu_u/sze_20.htm

14. Долбнєва, Д. В. (2019). Шляхи трансформації системи боротьби з економічними злочинами в Україні з урахуванням досвіду країн Європейського союзу. *ScienceRise, 2-3*(55-56), 21–27. https://doi.org/10.15587/2313-8416.2019.165337

15. ДТЕК. (2025). *Органи корпоративного управління*. https://dtek.com/content/files/organi-korporativnogo-upravlinnya.pdf

16. Дубініна, М. В., Сирцева, С. В., & Янковська, Т. Ю. (2019). Форензік як метод розслідування внутрішньокорпоративних випадків шахрайства. *Бухгалтерський облік, аналіз та аудит, 38*, 377–383.

17. Дубцов, Д., & Борківець, І. (2024). Шахрайство проти бізнесу: види та ефективне реагування. https://biz.ligazakon.net/analitycs/226314_shakhraystvo-proti-bznesu-vidi-ta-efektivne-reaguvannya

18. Дячкіна, А. (2024). Із початку року в Україні відкрили рекордну кількість справ про шахрайство. *Економічна правда*. https://www.epravda.com.ua/news/2024/04/19/712627/

19. Зайченко, К. С., & Діма, Н. І. (2021). Економічна безпека підприємства: сутність та роль. *Ефективна економіка, 5*. https://doi.org/10.32702/2307-2105-2021.5.90

20. Іванков, В. М. (2022). Генезис судової економічної експертизи. *Науковий вісник Льотної академії. Серія: Економіка, менеджмент та право, 7*, 13–21.

21. Іванов, С. В., & Чехунова (Мисник), К. П. (2024). Цифровий форензік як сучасний інструмент забезпечення економічної безпеки підприємств. *Економічний вісник Донбасу, 1-2*(75-76), 4–13. https://doi.org/10.12958/1817-3772-2024-1-2(75-76)-4-13

22. Климко, Т. Ю., & Мельник, О. О. (2015). Удосконалення роботи внутрішнього аудиту для запобігання фродів на підприєм-

стві. *Науковий вісник Міжнародного гуманітарного університету. Серія: Економіка і менеджмент, 13*, 251–254.

23. Ковальська, Л., Голій, О., & Голій, В. (2023). Економічна безпека підприємства: сутність, структура та механізм забезпечення. *Економічний форум, 1*(1), 126–137. https://doi.org/10.36910/6775-2308-8559-2023-1-16

24. Колодяжна, І. В., & Букріна, К. А. (2019). Економічна безпека в системі сталого функціонування підприємства. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство, 23*(1), 135–140.

25. Корнієнко, Т. О. (2022). Аналіз стану економічної безпеки України та пріоритети її зміцнення. *Економіка та суспільство, 28*. https://doi.org/10.32782/2524-0072/2022-38-61

26. Критенко, О. О., & Даньшина, Ю. В. (2015). Функціональний підхід до розкриття сутності інституціонального механізму державного управління системою державних закупівель. *Ефективність державного управління, 42*, 198–206.

27. Кудрейко, О. М. (2014). Інституційний механізм регулювання модернізації ринку освітніх послуг. *Наукові праці: Державне управління, 220*(242), 80–85.

28. Кургузенкова, Л. А. (2016). Економічна безпека підприємства: сутність та чинники формування її відповідного рівня. *Економічний вісник Запорізької державної інженерної академії, 2*, 29–33.

29. Мельничук, І. (2021). Форензік як форма попередження фінансових правопорушень. *Економіка та суспільство, 25*. https://doi.org/10.32782/2524-0072/2021-25-42

30. Мисник, К. (2021). Особливості розвитку системи економічних злочинів у сфері господарської діяльності: досвід Польщі. В *Science and Technology: Abstracts of the 24th International Scientific and Practical Conference* (с. 39–43). Lublin: Myśl Naukowa.

31. Мисник, К. (2021). Форензік у системі фінансово-економічної безпеки суб'єктів господарювання. В *Соціально-економічний розвиток і безпека України: стан та перспективи: матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених* (с. 184–187). Львів: Галицька видавнича спілка.

32. Мисник, К. П. (2020). Аналітична оцінка показників адміністративних правопорушень в Україні. В *Економіка та сучасний менеджмент: теоретичні підходи та практичні аспекти розви-*

тку: збірник матеріалів Всеукраїнської науково-практичної конференції (с. 37–40). Київ: Київський економічний науковий центр.

33. Мисник, К. П. (2020). Глобальні тенденції економічних злочинів у сфері господарської діяльності. В *Topical issues of science and practice: The VII International scientific and practical conference* (с. 121–124). London: International Science Group. https://doi.org/10.46299/ISG.2020.II.VII

34. Мисник, К. П. (2020). Інституційні умови забезпечення розвитку системи економічних розслідувань на підприємствах. В *Економіка сьогодні: проблеми моделювання та управління: матеріали X Міжнародної науково-практичної інтернет-конференції* (с. 238–240). Полтава: ПУЕТ.

35. Мисник, К. П. (2020). Особливості форензіку як методу економічних розслідувань на підприємствах України. В *Теоретичні та практичні питання узгодження інтересів розвитку територіальної системи: матеріали Всеукраїнської науково-практичної інтернет-конференції* (с. 60–63). Харків: Харківський національний університет імені В. Н. Каразіна.

36. Мисник, К. П. (2020). Сутність і особливості форензіку. В *Modern problems in science: The VIII International scientific and practical conference* (с. 96–100). Prague: International Science Group. https://doi.org/10.46299/ISG.2020.II.VIII

37. Мисник, К. П. (2021). Розвиток системи економічних злочинів у сфері господарської діяльності: особливості Німеччини, Польщі та Франції. В *Управління економікою: теорія та практика. Чумаченківські читання: збірник наукових праць* (с. 148–163). Київ: Інститут економіки промисловості НАН України. https://doi.org/10.37405/2221-1187.2021.148-163

38. Мисник, К. П. (2021). Сутність економічної безпеки суб'єктів господарювання. В *Проблеми планування в ринкових умовах: тези доповідей XX Міжнародної науково-практичної конференції* (с. 53–55). Хмельницький: Хмельницький національний університет.

39. Мисник, К. П. (2021). Формування організаційно-економічного механізму попередження економічних злочинів на підприємствах. В *Фінансова розвідка в Україні: збірник матеріалів науково-практичного семінару* (с. 91–94). Львів: Львівський державний університет внутрішніх справ.

40. Мисник, К. П. (2022). Форензік як стратегічний вектор модернізації національної економіки. В *Theoretical and science bases of actual tasks: Proceedings of the XIV International Scientific and Practical Conference* (с. 112–116). Lisbon: International Science Group. https://doi.org/10.46299/ISG.2022.1.14

41. Мисник, К. П. (2023). Розслідування економічних злочинів: сутність, ознаки та види. В *Реформування міжнародних економічних відносин і світового господарства в сучасних умовах: збірник матеріалів Міжнародної науково-практичної конференції* (с. 78–81). Ужгород: Ужгородський національний університет.

42. Мисник, К. П. (2024). Інтеграція механізму цифрового економічного форензіку в систему управління підприємствами. *Економіка промисловості, 2*(106), 64–76. https://doi.org/10.15407/econindustry2024.02.064

43. Мунтіян, В. (2015). *Економічна безпека України*. Київ: Лібра, 462 с.

44. Назарова, К. О., Нежива, М. О., Лосіцька, Т. І., Міняйло, В. П., & Новікова, Н. Л. (2021). Форензік-аудит як імператив економічної безпеки та розвитку компанії в умовах глобальних трансформацій. *Financial and Credit Activity Problems of Theory and Practice, 4*(35), 99–106. https://doi.org/10.18371/fcaptp.v4i35.221808

45. Нестеренко, О. (2024). Форензік-аудит як ефективний засіб протидії внутрішньокорпоративному шахрайству в умовах війни. *Acta Academiae Beregsasiensis. Economics, 5*, 392–405. https://doi.org/10.58423/2786-6742/2024-5-392-405

46. Новікова, О. Ф., & Покотиленко, Р. В. (2006). *Економічна безпека: концептуальне визначення та механізм забезпечення*. Донецьк: Інститут економіки промисловості НАН України, 408 с.

47. Новікова, О. Ф., Остафійчук, Я. В., Азьмук, Н. А., Панькова, О. В., Новак, І. М., & Касперович, О. Ю. (2025). Трудоресурсне забезпечення економічної безпеки на засадах стійкості. *Вісник економічної науки України, 1*(48), 114–124. https://doi.org/10.37405/1729-7206.2025.1(48).114-124

48. Опендатабот. (2024). Понад тисячу вироків за шахрайство вже винесено у 2024 році: як вберегти себе від шахраїв? https://opendatabot.ua/analytics/fraud-lessor

49. Опендатабот. (2024а). Кількість справ про шахрайство сягла історичного максимуму у 2023 році. https://opendatabot.ua/analytics/fraud-2023

50. Опендатабот. (2024b). Понад тисячу вироків за шахрайство вже винесено у 2024 році: як вберегти себе від шахраїв? https://opendatabot.ua/analytics/fraud-2024-5

51. Пабат, О. (2012). *Економічна безпека держави: інноваційні фактори*. Львів: Інститут регіональних досліджень НАН України, 168 с.

52. Павленко, Т. С., & Михайленко, О. В. (2017). Виявлення та попередження шахрайства як недооцінене завдання внутрішнього аудиту. *Бухгалтерський облік, аналіз та аудит, 8*, 197–200.

53. Підоричева, І. Ю. (2023). Оцінка галузевих диспропорцій, пов'язаних із потребами інноваційної трансформації підприємницького сектору України. *Економіка промисловості, 3*(103), 64–91. https://doi.org/10.15407/econindustry2023.03.064

54. Пілецька, С. Т., & Колесников, С. О. (2025). Математичне моделювання виявлення фінансових порушень у системі економічного форензіка для забезпечення безпеки підприємства в умовах цифрової економіки. *Вісник економічної науки України*, *1*(48), 165–169. https://doi.org/10.37405/1729-7206.2025.1(48).165-169

55. Попов, Е. В., & Семячков, К. А. (2018). Проблеми економічної безпеки цифрового суспільства в умовах глобалізації. *Економіка регіонів, 4*, 1088–1101.

56. Портал відкритих даних. (2025). https://data.gov.ua

57. Роїк, О. (2019). Шахрайство на підприємстві: як власникові захистити свій бізнес. *Юрист&Закон, 9*. https://www.asterslaw.com/ua/press_center/publications/corporate_fraud_how_owners_can_protect_their_business/

58. Рябчук, О. Г., & Твердун, С. О. (2021). Форензік як інструмент протидії економічним злочинам та фінансовому шахрайству на підприємстві. *Науковий вісник Ужгородського національного університету, 40*, 77–83. http://www.visnyk-econom.uzhnu.uz.ua/archive/40_2021ua/16.pdf

59. Самборський, О. В. (2023). Форензік-аудит у виявлені та запобіганні шахрайству. В *Облік, аналіз, аудит, оподаткування та фінансовий моніторинг в умовах повоєнного відновлення України: збірник матеріалів IX Міжнародної науково-практичної конференції* (с. 202–204). Київ: КНЕУ.

60. Семенець, А. О. (2019). Форензік аудит як ефективний засіб антикризового управління торговельною діяльністю. *Бізнес Інформ*, *4*(495), 280–287. https://doi.org/10.32983/2222-4459-2019-4-280-287

61. Семеног, А. Ю., Чухно, Р. Ю., Нейман, Є. В., & Кайлюк, О. Г. (2024). Теоретичні аспекти впливу цифрової трансформації на фінансову стійкість банків. *Цифрова економіка та економічна безпека, 3*(12), 69–75. https://doi.org/10.32782/dees.12-12

62. Сирцева, С. В., Недбайло, К. Г., & Янковська, Т. Ю. (2019). Поняття та види форензік-аудиту. В *Обліково-аналітичне і фінансове забезпечення діяльності суб'єктів господарювання: національні, глобалізаційні, євроінтеграційні аспекти: матеріали 4 Міжнародної науково-практичної інтернет-конференції* (с. 64–67). Миколаїв: МНАУ.

63. Сметанко, О. В. (2015). Становлення та розвиток внутрішнього аудиту в акціонерних товариствах України (Автореферат дисертації доктора економічних наук, спеціальність 08.00.09). Київський національний економічний університет імені Вадима Гетьмана, 33 с.

64. Стецюк, О. Я., & Чубай, В. М. (2023). Способи запобігання та виявлення фінансового шахрайства на підприємстві. *Молодий вчений, 3*(115), 120–127. https://doi.org/10.32839/2304-5809/2023-3-115-23

65. Титова, Ю. В. (2023). Форензік-аудит, як невід'ємна частина сучасної стратегії боротьби з фінансовими злочинами. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення, 82*. http://www.konferenciaonline.org.ua/ua/article/id-1418/

66. Тютченко, С. М. (2021). Функції форензіку як інструменту упередження корпоративного шахрайства та підвищення економічної безпеки підприємств. *Ефективна економіка, 5*. http://www.economy.nayka.com.ua/pdf/5_2021/101.pdf

67. Ульяненко, В. (2024). Скільки вироків за шахрайство вже винесено у 2024 році: приголомшлива цифра. https://glavcom.ua/country/society/skilki-virokiv-za-shakhrajstvo-vzhe-vineseno-u-2024-rotsi-priholomshliva-tsifra-1000379.html

68. Урба, С. І., & Івончак, І. О. (2018). Економічна безпека підприємництва як об'єкт теоретико-методологічного аналізу. *Держава та регіони. Серія: Економіка та підприємництво, 4*, 78–86.

69. Федорчак, О. (2017). Інституційний механізм державного управління. *Ефективність державного управління, 1*(50), 53–63.

70. Хамига, Ю. Я. (2020). Фінансове шахрайство: критерії ідентифікації та напрями мінімізації (Дисертація доктора філософії, спеціальність 072). Західноукраїнський національний університет, 308 с.

71. Харазішвілі, Ю. М. (2019). *Системна безпека сталого розвитку: інструментарій оцінки, резерви та стратегічні сценарії реалізації*. Київ: Інститут економіки промисловості НАН України, 304 с.

72. Хеленюк, М. (2021). Форензік: європейський досвід vs. українські реалії. *Юридична газета, 8*(738). https://yur-gazeta.com/publications/practice/korporativne-pravo-ma/forenzik-evropeyskiy-dosvid-vs-ukrayinski-realiyi.html

73. Чехунова (Мисник), К. П. (2024). Визначення економічного форензіку з позицій економічної безпеки. *Наукові перспективи, 7*(49), 870–883. https://doi.org/10.52058/2708-7530-2024-7(49)-870-883

74. Чехунова, К. П. (2024). Концептуальний підхід до оцінювання економічного ефекту від впровадження цифрового економічного форензіку. *Економіка. Фінанси. Право, 7*, 94–101. https://doi.org/10.37634/efp.2024.7.19

75. Чут, М. А. (2020). Використання інструментів форензік для забезпечення максимальної вартості виробничого підприємства. *Економіка та держава, 12*, 145–152. https://doi.org/10.32702/2306-6806.2020.12.145

76. Шикун, В., & Булик, Д. (2023). Фінансове шахрайство на підприємствах та методи його запобігання. *Економічний часопис Волинського національного університету імені Лесі Українки, 1*, 70–79. https://doi.org/10.29038/2786-4618-2023-01-70-79

77. Штулер, І. Ю., & Шевченко, Д. В. (2020). Сутність економічної безпеки та її система управління. *Актуальні проблеми економіки, 11*(233), 59–71.

78. Akinbi, A., MacDermott, Á., & Ismael, A. (2022). A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. *Forensic Science International: Digital Investigation, 42–43*, 301470. https://doi.org/10.1016/j.fsidi.2022.301470

79. American Academy of Forensic Sciences. (2024). About the AAFS. https://www.aafs.org/about-us

80. Association of Certified Fraud Examiners. (2016). The fraud tree: Occupational fraud and abuse classification system. https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/-/media/51fb0e7892e24fc392ed325fe0a42c2a.ashx

81. Association of Certified Fraud Examiners. (2020). *Report to the nations: 2020 global study on occupational fraud and abuse*. https://acfe-public.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

82. Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

83. Baldwin, D. A. (1997). The concept of security. *Review of International Studies, 23*(1), 5–26. https://doi.org/10.1017/S0260210597000053

84. Brennan, N., & Hennessy, J. (2001). Forensic accounting and the calculation of personal injury damages. *Bar Review, 6*, 533–539.

85. Brinson, A., Robinson, A., & Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investigation, 3*(Suppl.), S37–S43. https://doi.org/10.1016/j.diin.2006.06.008

86. Buzan, B. (2007). *People, states and fear: An agenda for international security studies in the post-Cold War era* (2nd ed.). ECPR Press, 318 p.

87. Carrier, B. (2003). Defining digital forensic examination and analysis tools. *International Journal of Digital Evidence, 1*(4), 1–12.

88. Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. *Proceedings of the Digital Forensic Research Conference (DFRWS)*. https://dfrws.org/wp-content/uploads/2019/06/2004_USA_paper-an_event-based_digital_forensic_investigation_framework.pdf

89. Casey, E. (Ed.). (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Elsevier, 837 p.

90. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

91. Cellebrite. (2023). Mobile device forensics. https://cellebrite.com/en/digital-forensics/mobile-device-foren-sics/

92. Coase, R. (1992). The institutional structure of production. *American Economic Review, 82*(4), 713–719.

93. Collier, P. A., & Spaul, B. J. (1992). A forensic methodology for countering computer crime. *Artificial Intelligence Review, 6*(2), 203–215. https://doi.org/10.1007/BF00150234

94. Connor, J. M. (2007). Forensic economics: An introduction with special emphasis on price fixing. *Journal of Competition Law and Economics, 4*(1), 31–59. https://doi.org/10.1093/joclec/nhm022

95. Council of Europe. (2004). *Convention on cybercrime*. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

96. Cressey, D. R. (1953). *Other people's money: A study of the social psychology of embezzlement*. Free Press, 191 p.

97. Deloitte. (2025). Фінансові розслідування (форензік). https://www2.deloitte.com/ua/uk/pages/financial-services/solutions/forensic-in-Ukraine.html

98. Dent, C. M. (2001). Singapore's foreign economic policy: The pursuit of economic security. *Contemporary Southeast Asia, 23*(1), 1–23. https://doi.org/10.1355/CS23-1A

99. Di Tella, R., & Schargrodsky, E. (2003). The role of wages and auditing during a crackdown on corruption in the city of Buenos Aires. *Journal of Law and Economics, 46*(1), 269–292. https://doi.org/10.1086/345578

100. Diaz, L. O. (2023). What can digital forensics do for my business? Ten Intelligence Limited. https://tenintel.com/what-can-digital-forensics-do-for-my-business/

101. Dreyer, K. (2014). A history of forensic accounting (Honors Projects, 296). Grand Valley State University, 23 p.

102. Ebrahimi, S., & Eshghi, K. (2022). A meta-analysis of the factors influencing the impact of security breach announcements on stock returns of firms. *Electronic Markets, 32*(1), 1–24. https://doi.org/10.1007/s12525-022-00550-2

103. ECS Infotech. (2024). Trusted hard drive forensic data recovery services. https://www.ecsinfotech.com/disk-foren-sics/

104. Edelman, B. G., & Larkin, I. (2015). Social comparisons and deception across workplace hierarchies: Field and experimental evidence. *Organization Science, 26*(1), 78–98. https://doi.org/10.1287/orsc.2014.0942

105. Edwards, K. A., & Murphy, G. (2022). Addressing economic insecurity in the U.S. National Academy of Social Insurance. https://www.nasi.org/research/economic-security/the-four-pillars-of-economic-security/

106. Ernst & Young. (2025). Форензік послуги. https://www.ey.com/uk_ua/assurance/forensic-integrity-service-offerings

107. Ewald, C., Hüschelrath, K., & Schweitzer, H. (2014). Best practices for expert economic opinions – Key element of forensic economics in competition law. In K. Hüschelrath & H. Schweitzer (Eds.), *Public and private enforcement of competition law in Europe* (pp. 141–166). Springer. https://doi.org/10.1007/978-3-662-43975-3_9

108. Fischer, C. C. (2006). The valuation of household production: Divorce, wrongful injury and death litigation. *American Journal of Economics and Sociology, 53*(2), 187–199. https://doi.org/10.1111/j.1536-7150.1994.tb02585.x

109. Fortra. (2024). 130 cyber security statistics: 2024 trends and data. https://www.terranovasecurity.com/blog/cyber-security-statistics

110. Furubotn, E. G., & Richter, R. (1997). *Institutions and economic theory*. University of Michigan Press, 542 p.

111. Galbraith, C., Smyth, P., & Stern, H. (2020). Quantifying the association between discrete event time series with applications to digital forensics. *Journal of the Royal Statistical Society: Series A (Statistics in Society), 183*(3), 1005–1027. https://doi.org/10.1111/rssa.12549

112. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*(Suppl.), S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

113. Goel, S., & Shawky, H. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404–410. https://doi.org/10.1016/j.im.2009.06.005

114. Government of Canada Publications. (2024). Computer crime (BP-87E). https://publications.gc.ca/Collection-R/LoPBdP/BP/bp87-e.htm

115. Guo, H., & Tang, Z. (2025). Artificial Intelligence in Forensic Accounting: A Literature Review. *Journal of Accounting and Finance, 25*(3). https://doi.org/10.33423/jaf.v25i3.7888

116. Hacker, J. S. (2009). Economic security. In J. Stiglitz, J. Fitoussi, & M. Durand (Eds.), *For good measure: Advancing research on well-being metrics beyond GDP* (pp. 203–240). OECD Publishing. https://doi.org/10.1787/9789264307278-10-en

117. Hirschman, A. O. (1945). *National power and the structure of foreign trade*. University of California Press, 194 p. https://doi.org/10.1016/j.im.2009.06.005

118. Horsman, G., & Sunde, N. (2022). Unboxing the digital forensic investigation process. *Science & Justice, 62*(2), 171–180. https://doi.org/10.1016/j.scijus.2022.01.002

119. Hughes, G. (1991). Computer crime: The liability of hackers. https://classic.austlii.edu.au/au/journals/ANZCompuLawJl/1991/6.pdf

120. IBM Security Systems. (2012). *IBM X-Force 2012 trend and risk report*. https://www.ibm.com/ibm/files/I218646H25649F77/Risk_Report.pdf

121. International Labour Organization. (2004). Definitions: What we mean when we say "economic security". In *Economic security for a better world*. https://webapps.ilo.org/public/english/protection/ses/download/docs/definition.pdf

122. Interpol. (2021). *Guidelines for digital forensics first responders: Best practices for search and seizure of electronic and digital evidence*. https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf

123. Ireland, T. R. (2001). Categories of time use for forensic economics. *Journal of Forensic Economics, 14*(1), 23–34. https://doi.org/10.5085/0898-5510-14.1.23

124. Irons, A. D., Stephens, P., & Ferguson, R. I. (2009). Digital investigation as a distinct discipline: A pedagogic perspective. *Digital Investigation, 6*(1–2), 82–90. https://doi.org/10.1016/j.diin.2009.05.002

125. Jenks, J. W. (1888). The Michigan Salt Association. *Political Science Quarterly, 3*(1), 78–98. https://doi.org/10.2307/2138986

126. Juma'h, A., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting and Information Management, 28*(2), 275–301. https://doi.org/10.1108/IJAIM-01-2019-0006

127. Kalbande, D., & Jain, N. (2013). Comparative digital forensic model. *International Journal of Innovative Research in Science, Engineering and Technology, 2*(8), 3414–3419.

128. Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69–91. https://doi.org/10.2753/JEC1086-4415120103

129. Khalymon, S., Polovnikov, V., Kravchuk, O., Marushchak, O., & Strilets, O. (2019). Forensic economic examination as a means of investigation and counteraction of economic crimes in East Europe (Example of Ukraine). *Journal of Legal, Ethical and Regulatory Issues, 22*(3), 1–8.

130. Kim, Y., & Kim, K. J. (2010). A forensic model on deleted-file verification for securing digital evidence. *2010 International*

Conference on Information Science and Applications, 1–8. https://doi.org/10.1109/ICISA.2010.5480346

131. Kimmons, J. (2023). Digital evidence, data recovery, and forensic analysis techniques. https://kimmonsinv.com/digital-evidence-data-recovery-and-forensic-analysis-techniques/

132. Knight, B. (2006). Are policy platforms capitalized into equity prices? Evidence from the Bush/Gore 2000 Presidential Election. *Journal of Public Economics, 90*(4–5), 751–773. https://doi.org/10.1016/j.jpubeco.2005.06.003

133. Ko, M., & Dorantes, A. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, *17*(2), 13–22.

134. KPMG. (2024). Форензік. https://kpmg.com/ua/uk/home/services/consulting/forensic.html

135. KPMG. (2024a). Форензік-ІТ. https://kpmg.com/ua/uk/home/services/consulting/forensic/forensic-it.html

136. Lajeunesse, R. M. (2015). Institutionalist method and forensic proof. In M. D. White (Ed.), *Law and social economics: Essays in ethical values for theory, practice, and policy* (pp. 61–73). Palgrave Macmillan.

137. Landmann, J. (2019). The impact of data security on firm value: How do stock markets react to data breach announcements? (Master's dissertation, Universidade Católica Portuguesa). https://repositorio.ucp.pt/bitstream/10400.14/26875/1/152417068%20Juliane%20Landmann%20W%20PDFA.pdf, 46 p.

138. Legislation.gov.uk. (1990). *Computer Misuse Act 1990*. https://www.legislation.gov.uk/ukpga/1990/18/contents

139. Lianos, I. (2012). The emergence of forensic economics in competition law: Foundations for a sociological analysis (CLES Working Paper Series 5/2012). Centre for Law, Economics and Society, 41 p. https://doi.org/10.2139/ssrn.2197025

140. Montasari, R. (2017). A standardised data acquisition process model for digital forensic investigations. *International Journal of Information and Computer Security, 9*(3), 229–249. https://doi.org/10.1504/IJICS.2017.085139

141. Musca Law. (2023). Florida cybercrime laws: Offenses, punishments, and potential defenses. https://www.muscalaw.com/blog/florida-cybercrime-laws-offenses-punishments-and-potential-defenses

142. Mysnyk, K. (2023). Analysis of risk assessment methods in the field of economic activity of enterprises. In *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку: матеріали XXXI Міжнар. наук.-практ. конф.* (pp. 440–446). Kyiv: ГО «ВАДНД».

143. Mysnyk, K. (2023). The essence of the concept of "economic crime". In *Scientific method: Reality and future trends of researching: Collection of scientific papers «SCIENTIA» with proceedings of the I International Scientific and Theoretical Conference* (pp. 14–16). Zagreb: European Scientific Platform.

144. National Institute of Standards and Technology. (2024). Computer forensics tool testing program (CFTT). https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

145. North, D. C. (1992). Institution, ideology and economic performance. *Cato Journal*, *11*(3), 477–499.

146. Onyshchenko, S., Maslii, O., & Ivanyuk, B. (2019). The impact of external threats to the economic security of the business. *Proceedings of the 2019 7th International Conference on Modeling, Development and Strategic Management of Economic System*, 156–160. https://doi.org/10.2991/mdsmes-19.2019.30

147. Palmer, G. (2001). A road map for digital forensic research (Technical Report DTR-T001-01). Digital Forensic Research Workshop. https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

148. Parker, D. (1976). *Crime by computer*. Scribner, 308 p.

149. Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security*, *9*(8), 38–44.

150. Pollitt, M. M. (1995). Computer forensics: An approach to evidence in cyberspace. *Proceedings of the National Information Systems Security Conference*, 487–491.

151. Ponemon Institute. (2012). *The human factor in data protection*. https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf

152. Porter, R. H., & Zona, J. D. (1993). Detection of bid rigging in procurement auctions. *Journal of Political Economy*, *101*(3), 518–538. https://doi.org/10.1086/261885

153. PricewaterhouseCoopers. (2020). *PwC's global economic crime and fraud survey 2020*. https://www.pwc.com/ua/en/survey/2020/economic-crime-survey.html

154. PricewaterhouseCoopers. (2020a). Всесвітнє дослідження економічних злочинів та шахрайства 2020: результати опитування українських організацій. Виведення шахрайства з тіні. https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf, 25 p.

155. PricewaterhouseCoopers. (2021). Interview with Dmytro Nechytailo (Partner, Advisory Leader at PwC Ukraine). https://www.pwc.com/ua/en/press-room/2021/dmytro-nechytailo-interview.html

156. PricewaterhouseCoopers. (2024). *PwC's global economic crime survey 2024*. https://www.pwc.com/gx/en/services/forensics/gecs/2024-global-economic-crime-survey.pdf

157. PricewaterhouseCoopers. (2024a). Всесвітнє дослідження економічних злочинів і шахрайства 2024. Результати опитування українських компаній. https://www.pwc.com/ua/uk/survey/2024/gecs 2024-ukr.pdf

158. PricewaterhouseCoopers. (2024b). Форензік-діагностика. https://www.pwc.com/ua/uk/services/forensic/forensic-health-check.html

159. PricewaterhouseCoopers. (2025). Управління ризиками шахрайства. https://www.pwc.com/ua/uk/services/forensic/fraud-risk-management.html

160. Public Company Accounting Oversight Board. (2002). *Consideration of fraud in a financial statement audit* (AU §316). https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/au-00316.pdf

161. Rashid, M. A., Al-Mamun, A., Roudaki, H., & Yasser, Q. (2022). An overview of corporate fraud and its prevention approach. *Australasian Business, Accounting and Finance Journal*, *16*(1), 101–118. https://doi.org/10.14453/aabfj.v16i1.7

162. Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*, *6*, 100313. https://doi.org/10.1016/j.fsisyn.2022.100313

163. Ribaux, O., Baechler, S., & Rossy, Q. (2022). Forensic intelligence and traceology in digitalised environments: The detection and analysis of crime patterns to inform practice. In M. Gill (Ed.), *The handbook of security* (pp. 81–100). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-91735-7_5

164. Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law, 1*(2), 19–38. https://doi.org/10.15394/jdfsl.2006.1004

165. Ronis, S. R. (Ed.). (2011). *Economic security: Neglected dimension of national security?* Center for Strategic Conferencing, Institute for National Strategic Studies, 130 p. https://doi.org/10.21236/ADA585192

166. SalvationDATA. (2023). What is database forensics? https://www.salvationdata.com/knowledge/what-is-database-foren-sics/

167. Samoilenko, Y., Britchenko, I., Levchenko, I., Lošonczi, P., Bilichenko, O., & Bodnar, O. (2022). Economic security of the enterprise within the conditions of digital transformation. *Economic Affairs, 67*(4), 619–629. https://doi.org/10.46852/0424-2513.4.2022.28

168. Schap, D. (2010). Forensic economics: An overview. *Eastern Economic Journal, 36*(3), 347–352. https://doi.org/10.1057/eej.2010.27

169. Schinkel, M. P. (2008). Forensic economics in competition law enforcement. *Journal of Competition Law & Economics, 4*(1), 1–30. https://doi.org/10.1093/joclec/nhm033

170. Shakeel, I. (2015). *Introduction to computer forensics and digital investigation*. Infosec Institute, 79 p.

171. Šimašius, R., & Vilpišauskas, R. (2005). The concept of economic security and the principles of economic security policy in Lithuania. *Lithuanian Annual Strategic Review, 3*(1), 249–266. https://doi.org/10.47459/lasr.2005.3.12

172. Singleton, T., Singleton, A., Bologna, J., & Lindquist, R. (2006). *Fraud auditing and forensic accounting* (3rd ed.). John Wiley & Sons, 338 p.

173. Sjouwerman, S. (2020). Stanford research: 88% of data breaches are caused by human error. https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error

174. Smelik, R. (2020). Economic security of the organisation: Financial component management. *Financial Law Review, 18*(2), 32–47. https://doi.org/10.4467/22996834FLR.20.008.12430

175. Snyder, C. M., & Zidar, O. M. (2011). Resume padding among economists. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1986219

176. Stiglitz, J. E., Fitoussi, J., & Durand, M. (Eds.). (2018). *For good measure: Advancing research on well-being metrics beyond GDP*. OECD Publishing. https://doi.org/10.1787/9789264307278-en

177. Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review, 5*(1), 1–12. https://doi.org/10.2307/2083937

178. Syifaurachman, S. (2025). Opportunities and Challenges of Artificial Intelligence in Digital Forensics. *International Journal Software Engineering and Computer Science*, 5(2), 560–575. https://doi.org/10.35870/ijsecs.v5i2.4371

179. Tinari, F. D. (2001). Teaching forensic economics in the university curriculum. *Journal of Forensic Economics, 14*(3), 243–260.

180. Tinari, F. D. (Ed.). (2016). *Forensic economics: Assessing personal damages in civil litigation*. Palgrave Macmillan, 327 p. https://doi.org/10.1057/978-1-137-56392-7

181. Tosun, O. K. (2018). Cyber-attacks and stock market activity. *International Review of Financial Analysis, 76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795

182. Tunggal, A. T. (2024). What is digital forensics? https://www.upguard.com/blog/digital-foren-sics

183. United Nations Development Programme. (1994). *Human development report 1994*. https://doi.org/10.18356/87e94501-en

184. Vacca, J. R. (2005). *Computer forensics: Computer crime scene investigation* (2nd ed.). Charles River Media, 832 p.

185. Valeriu, I., & Diamescu, A. (2010). Some opinions on the relation between security economy and economic security. *Romanian Journal of Economics, 40*(2), 122–159.

186. Varol, A., & Sonmez, Y. U. (2021). Review of evidence collection and protection phases in digital forensics process. *International Journal of Information Security Science, 6*(4), 39–46.

187. Viancourt, P. E. (2021). Data breach announcements: Evaluating the content and timing of breach announcements and their effect on firm value (Doctoral dissertation, Rollins College). https://scholarship.rollins.edu/dba_dissertations/38, 117 p.

188. Wakefield, J. (2014). eBay faces investigations over massive data breach. BBC News. https://www.bbc.com/news/technology-27539799

189. Wells, J. T. (2007). *Corporate fraud handbook: Prevention and detection* (4th ed.). John Wiley & Sons, 425 p.

190. Williamson, O. E. (1985). *The economic institutions of capitalism*. Free Press, 468 p.

191. Wolfers, A. (1952). "National security" as an ambiguous symbol. *Political Science Quarterly, 67*(4), 481–502. https://doi.org/10.2307/2145138

192. Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things, 19*, 100544. https://doi.org/10.1016/j.iot.2022.100544

193. Yeboah-Boateng, E. O. (2015). An assessment of corporate security policy violations using live forensics analysis. *International Journal of Cyber-Security and Digital Forensics, 4*(1), 262–271. https://doi.org/10.17781/P001385

194. Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science and Information Technology, 3*(3), 17–31. https://doi.org/10.5121/ijcsit.2011.3302

195. Zakaria, Z. N. Z., Che Hussain, N. H., Awang, Y., & Shuhidan, S. M. (2025). Smart Forensics: Tracing the Rise of Artificial Intelligence in Forensic Accounting, Fraud Detection and Risk Management. *Information Management and Business Review*, 17(2(I)S), 51–68. https://doi.org/10.22610/imbr.v17i2(I)S.4565

196. Zangana, H. M., Suryawati, R. F., Mustafa, F. M., & Vitianingsih, A. V. (2025). AI in Forensic Accounting: Detecting Anomalies and Financial Fraud Through Intelligent Systems. *In AI in Digital Forensics and Cybercrime Investigation: Methods, Ethics, and Emerging Technologies (pp. 125–162). IGI Global*. https://doi.org/10.4018/979-8-3373-6536-7.ch005

197. Zitzewitz, E. (2012). Forensic economics. *Journal of Economic Literature, 50*(3), 731–769. https://doi.org/10.1257/jel.50.3.731

Наукове видання

Чехунова Катерина Павлівна

ЕКОНОМІЧНИЙ ФОРЕНЗІК ЯК БЕЗПЕКОВА ІННОВАЦІЯ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВІЗАЦІЇ ТА РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Монографія

Оригінал-макет підготовлено у відділі інформатизації наукової діяльності ІЕП НАН України

Підписано до публікації 30.05.2026 р.
Об'єм даних *3,0* Мб.
Замовлення № 1553.

Видавець і виготовлювач
Інститут економіки промисловості
Національної академії наук України
вул. Марії Капніст, 2, м. Київ, 03057,
тел. (044) 200-55-71, E-mail: admin@econindustry.org