Фінанси, банківська справа, страхування та фондовий ринок

УДК 330.658.012

DOI https://doi.org/10.5281/zenodo.15795360

Роль великих даних у прогнозуванні загроз економічної безпеки підприємств в Україні

Фурса Тетяна Петрівна,
кандидат економічних наук, доцент, кафедра управління та адміністрування,
Івано-Франківський навчально-науковий інститут менеджменту,
Західноукраїнський національний університет, м. Івано-Франківськ, Україна,
https://orcid.org/0000-0003-4562-2252

Суліма Наталія Миколаївна,
кандидат економічних наук, доцент, доцент кафедри економіки,
Національний університет біоресурсів і природокористування України,
м. Київ, Україна, https://orcid.org/0000-0002-3852-7989

Василина Орися Романівна,
кандидат економічних наук, доцент, кафедра економіки,
Львівський національний університет ветеринарної медицини та
біотехнологій ім. С.З. Ґжицького, м. Дубляни, Україна,
https://orcid.org/0000-0003-2124-3792

Прийнято: 18.06.2025 | Опубліковано: 03.06.2025

Анотація. *У сучасних умовах економічна безпека підприємства є ключовою детермінантою його сталого розвитку та конкурентоспроможності, набуваючи особливого значення у контексті*

нестабільного зовнішнього середовища та конкуренції, характерних для трансформаційної економіки України. У період стрімких технологічних змін і зростаючих загроз як зовнішнього, так і внутрішнього характеру, підприємства змушені переосмислювати підходи до забезпечення своєї економічної безпеки.

***Метою статті** є обґрунтування доцільності використання великих даних як інструменту підвищення ефективності системи виявлення та прогнозування загроз економічній безпеці підприємств.*

***Методи.** У дослідженні використано комплекс методів, зокрема, збирання й порівняння інформації, а також методи аналізу, синтезу та узагальнення, які становлять методологічну основу роботи.*

***Результати.** Показано, що система економічної безпеки є не просто набором захисних заходів, а комплексною підсистемою функціонування сучасного підприємства, здатною забезпечити його життєздатність та досягнення стратегічних цілей. У роботі систематизовано основні загрози економічній безпеці, поділяючи їх на зовнішні та внутрішні. Кожна група загроз розглядається з конкретними прикладами, що дозволяє краще зрозуміти їх джерела та потенційний вплив на діяльність підприємства. Наголошується на провідній ролі цифрової трансформації бізнесу у зміцненні економічної безпеки. Впровадження передових технологій розглядається як інструмент для підвищення прозорості та контрольованості процесів прийняття рішень, що є критично важливим для запобігання внутрішнім загрозам. Центральне місце у дослідженні посідає аналіз технологій великих даних та прогнозної аналітики. Обґрунтовано, що ці технології надають підприємствам можливість у режимі реального часу збирати та аналізувати великі масиви інформації, передбачати зміни на ринку, виявляти потенційні фінансові й операційні ризики, адаптувати бізнес-моделі до потреб клієнтів, прогнозувати їх поведінку та ухвалювати стратегічно важливі управлінські рішення.*

ISSN: 2786-9431

Висновки. *Систематичне збирання, обробка та аналіз інформаційних потоків створює умови для більш точного передбачення фінансових, операційних та кіберзагроз. Завдяки впровадженню інструментів великих даних підприємства можуть оперативно реагувати на зміну зовнішнього середовища та уникати критичних втрат. Таким чином, аналітика великих даних сприяє прийняттю обґрунтованих управлінських рішень, що підвищує загальну стійкість бізнесу. Особливо актуальним це є для українських підприємств в умовах високої турбулентності ринку, воєнних дій та економічної нестабільності. Впровадження цифрових технологій відкриває нові можливості для побудови ефективної системи ризик-менеджменту.*

Ключові слова: *цифрові технології, аналітика даних, ризики, цифрова трансформація, дані у реальному часі.*

The role of big data in predicting threats to the economic security of enterprises in Ukraine

Tetiana Fursa,
PhD in Economics, Associate Professor, Department of Management and Administration, Ivano-Frankivsk Educational and Research Institute of Management, West Ukrainian National University, Ivano-Frankivsk, Ukraine, https://orcid.org/0000-0003-4562-2252

Nataliia Sulima,
PhD in Economics, Associate Professor of the Department of Economics, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine, https://orcid.org/0000-0002-3852-7989

Orysia Vasylyna,
PhD, Associate Professor, Department of Economy, Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies of Lviv, Dublyany, Ukraine, https://orcid.org/0000-0003-2124-3792

Abstract. *In modern conditions, the economic security of an enterprise is a key determinant of its sustainable development and competitiveness, acquiring particular importance in the context of the unstable external environment and competition characteristic of the transformational economy of Ukraine. In a period of rapid technological changes and growing threats of both external and internal nature, enterprises are forced to rethink approaches to ensuring their economic security.*

The ***article aims*** *to substantiate the feasibility of using big data to increase the system's efficiency in identifying and predicting threats to the economic security of enterprises.*

Methods. *The study used a set of methods, in particular, information collection and comparison, as well as methods of analysis, synthesis and generalization, constituting the work's methodological basis.*

Results. *It is shown that the economic security system is not just a set of protective measures but a complex subsystem of the functioning of a modern enterprise, capable of ensuring its viability and achieving strategic goals. The work systematizes the main threats to economic security, dividing them into external and internal. Each group of threats is considered with specific examples, which allows for a better understanding of their sources and potential impact on the enterprise's activities. The leading role of digital business transformation in strengthening economic security is emphasized. Introducing advanced technologies is considered a tool for increasing transparency and controllability of decision-making processes, which is critically important for preventing internal threats. The study focuses on the analysis of big data technologies and predictive analytics. It is substantiated that*

these technologies allow enterprises to collect and analyze large amounts of information in real-time, predict market changes, identify potential financial and operational risks, adapt business models to customer needs, predict their behavior and make strategically important management decisions.

Conclusions. *Systematic collection, processing and analysis of information flows create conditions for more accurate financial, operational and cyber threat prediction. Thanks to the introduction of big data tools, enterprises can quickly respond to changes in the external environment and avoid critical losses. Thus, big data analytics helps to make informed management decisions, increasing the business's overall stability. It is especially relevant for Ukrainian enterprises in high market turbulence, military operations, and conditions of economic instability. The introduction of digital technologies opens up new opportunities for building an effective risk management system.*

Keywords: *digital technologies, data analytics, risks, digital transformation, real-time data.*

Постановка проблеми. Сучасні підприємства функціонують у надзвичайно динамічному та нестабільному середовищі, що зумовлює постійне зростання ризиків, які загрожують їх економічній безпеці. В умовах глобалізації, цифрової трансформації економіки, гібридних загроз, кіберризиків і воєнної агресії проти України, питання економічної безпеки підприємств набуває особливої ваги. Традиційні підходи до оцінки ризиків і прогнозування кризових ситуацій часто є недостатньо ефективними для обробки великих обсягів даних, що постійно оновлюються у режимі реального часу. У цьому контексті впровадження технологій великих даних створює нові можливості для своєчасного виявлення небезпечних тенденцій, моделювання можливих сценаріїв розвитку подій та підвищення обґрунтованості управлінських рішень. Водночас в Україні досі недостатньо розроблені методологічні підходи щодо інтеграції великих даних у систему забезпечення

економічної безпеки підприємств, що обумовлює потребу у глибокому науковому дослідженні цієї проблематики.

Аналіз останніх досліджень і публікацій. Питання забезпечення економічної стабільності підприємств, зокрема, у контексті використання цифрових технологій, активно досліджується сучасними вітчизняними й зарубіжними науковцями. Так, Л. Петренко та П. Худіков [1] розглядають економічну безпеку як комплексний стан захисту підприємства від внутрішніх і зовнішніх загроз, підкреслюючи важливість системного підходу до оцінки ризиків. Н. Васюткіна та В. Ватащук акцентують увагу на необхідності адаптивних механізмів безпеки [2]. Д. Крилов [3] досліджує внутрішні і зовнішні загрози безпеці підприємств, наголошуючи на ролі моніторингу та прогнозування для своєчасного реагування.

Група вчених на чолі з О. Попело [4] досліджують вплив цифровізації на стратегію розвитку підприємства у контексті створення економічної безпеки. Автори визначили основні перешкоди, що стримують розвиток інноваційних технологій та цифрових платформ в Україні. В. Бакай [5] підкреслює, що цифрові технології є як інструментом підвищення безпеки, так і джерелом нових кіберзагроз, що вимагає комплексного підходу до управління ризиками. О. Вовк, О. Стець та І. Лазаренко [6] відзначають, що впровадження цифрових рішень дозволяє мінімізувати операційні ризики та підвищити ефективність захисту підприємств. Науковці акцентують увагу на важливості аналітики даних у процесах прогнозування ризиків та прийняття стратегічних управлінських рішень. С. Онищенко, С. Білько, А. Янко та С. Сівіцька [7] розглядають питання інформаційної безпеки бізнесу, акцентуючи увагу на сучасних викликах та технологічних рішеннях у контексті цифровізації підприємств. У статті подано інноваційні підходи до захисту бізнес-інформації, що дозволяють підвищити загальний рівень економічної безпеки підприємств у цифровому середовищі. Дослідження О. Остапчук та О. Баксалової [8] висвітлюють роль інноваційних управлінських технологій,

ISSN: 2786-9431

таких як блокчейн та автоматизація, у зміцненні економічної безпеки, одночасно звертаючи увагу на труднощі їх впровадження. О. Олійничук наголошує на необхідності інтеграції цифрових технологій у системи стратегічного управління ризиками для забезпечення безперервного контролю [9]. Однією з ключових передумов підвищення ефективності прогнозування загроз економічній безпеці підприємств є інтеграція технологій автоматизації обробки великих даних із системами штучного інтелекту та адаптивними інтерфейсами користувачів. Як зазначає Ю. Горбенко, поєднання AI-Powered UI Adaptation і Data Automation Frameworks створює умови для безперервного збору, класифікації та інтерпретації масивів даних у режимі реального часу, що критично важливо для оперативного реагування на ризики [18].

Огляд фахових джерел свідчить про зростаючу увагу наукової спільноти до проблеми інтеграції цифрових технологій, зокрема, великих даних, у процеси формування та зміцнення економічної безпеки підприємств в Україні.

Виділення невирішених раніше частин загальної проблеми. Попри наявність досліджень, присвячених теоретичним аспектам застосування технологій великих даних у бізнесі, досі недостатньо вивченими залишаються питання практичної інтеграції цих технологій у систему прогнозування загроз економічній безпеці підприємств. У цій статті прагнемо розкрити потенціал використання великих даних для своєчасного виявлення та нейтралізації загроз, що виникають у внутрішньому та зовнішньому середовищі підприємства.

Формулювання цілей статті (постановка завдання). Мета статті – проаналізувати потенціал використання технологій великих даних у процесі прогнозування загроз для економічної безпеки підприємств в Україні. Для досягнення цієї мети необхідно вирішити наступні завдання:

– охарактеризувати сутність економічної безпеки підприємства та систематизувати основні її завдання;

ISSN: 2786-9431

– класифікувати зовнішні та внутрішні загрози економічній безпеці підприємств;

– проаналізувати потенціал технологій великих даних та прогнозної аналітики як ефективних інструментів виявлення, оцінки та нейтралізації загроз економічній безпеці.

Виклад основного матеріалу дослідження. Незалежно від форми власності, типу чи напряму діяльності, кожен суб'єкт господарювання сьогодні функціонує в умовах нестабільного зовнішнього середовища та зростаючої конкуренції. У таких обставинах особливого значення набуває економічна безпека підприємства як важливий чинник стабілізації його фінансово-економічного стану та забезпечення досягнення стратегічних цілей бізнесу [6, с. 102].

Економічна безпека підприємства є ключовим чинником його стійкості, конкурентоспроможності та довгострокового розвитку, що набуває особливої ваги в умовах зростання як внутрішніх, так і зовнішніх загроз, характерних для трансформаційної економіки України. Як зазначають В. Васюткіна та В. Ватащук, економічна безпека завжди є важливою підсистемою функціонування підприємства, зокрема, в умовах жорсткої конкуренції та нестабільності ринкового середовища [2].

Проаналізувавши підходи різних науковців до структурування економічної безпеки підприємства, пропонуємо наступну систему її складових (табл. 1).

Таблиця 1

Складові економічної безпеки підприємства

Складова	Сутнісна характеристика
Фінансова	Відображає здатність підприємства ефективно використовувати фінансові ресурси, що проявляється у досягненні стабільних і високих фінансових показників діяльності
Техніко-технологічна	Характеризує рівень застосовуваних технологій. Передбачає впровадження інновацій з метою збереження конкурентоспроможності продукції та оптимізації витрат

ISSN: 2786-9431

Кадрово-інтелектуальна	Включає збереження, розвиток і ефективне використання кадрового та інтелектуального потенціалу підприємства, а також якісне управління персоналом
Політико-правова	Забезпечує правову стабільність діяльності підприємства шляхом дотримання чинного законодавства як самою організацією, так і її співробітниками
Екологічна	Полягає у дотриманні екологічних стандартів виробництва, мінімізації шкоди довкіллю та зниженні витрат, пов'язаних із негативним впливом на навколишнє середовище
Інтерфейсна	Визначає надійність і результативність взаємодії з контрагентами. Забезпечує привабливість підприємства та його продукції, зміцнення ринкових позицій

Джерело: узагальнено авторами на основі [1; 2; 3; 10]

Система економічної безпеки підприємства виконує низку важливих завдань, спрямованих на охорону інтересів компанії, моніторинг зовнішнього середовища, захист інформаційних ресурсів та формування позитивного іміджу (рис.1).

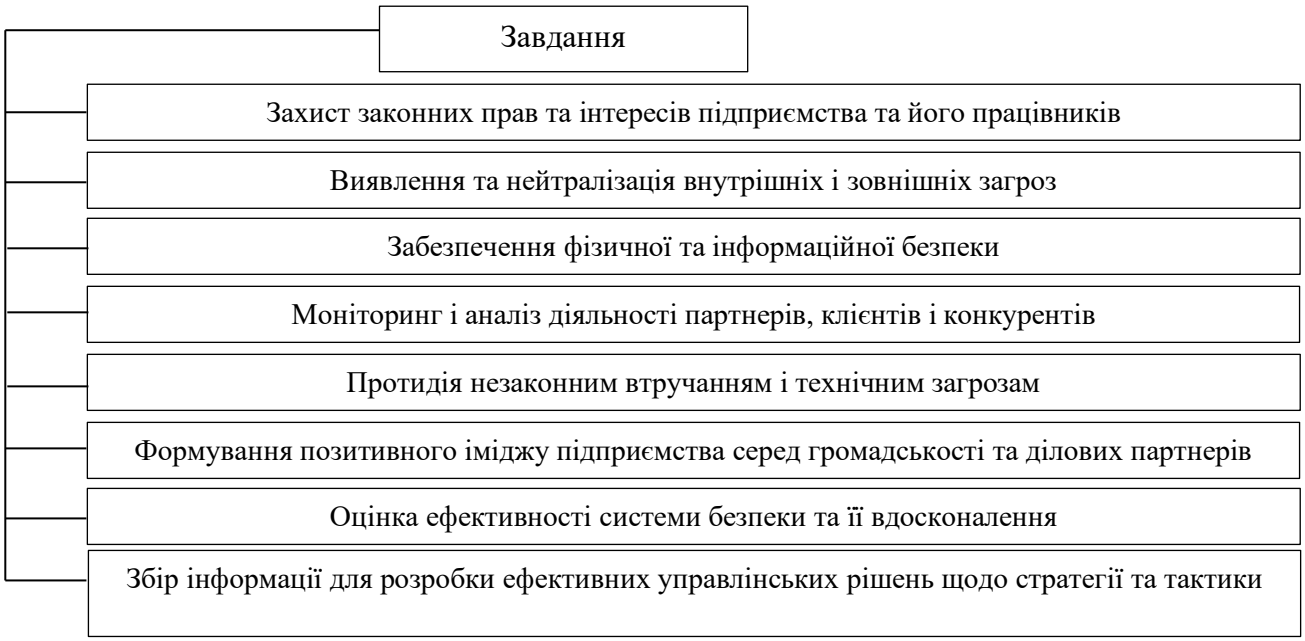

Рис.1. Завдання системи економічної безпеки підприємства

Джерело: систематизовано на основі [1, с. 796]

Зауважимо, що успішне функціонування підприємства залежить не лише від його внутрішніх ресурсів та управлінських рішень, а й від здатності

своєчасно реагувати на потенційні загрози, що можуть призвести до дестабілізації його фінансового, інформаційного, виробничого чи кадрового потенціалу. Загрози економічній безпеці є багатофакторними та можуть мати як зовнішнє, так і внутрішнє походження. Їх систематизація дозволяє краще розуміти джерела ризиків і формувати ефективну стратегію протидії (табл. 2).

Таблиця 2

Основні загрози економічній безпеці підприємств

Група загроз	Сфера впливу	Приклади конкретних загроз
Зовнішні загрози		
Економічні	Фінансова, ринкова	Інфляція, нестабільність валютного курсу, зростання податкового тиску
Політичні	Юридична, регуляторна	Зміни в законодавстві, політична нестабільність, воєнні дії
Технологічні	Виробнича, інноваційна	Технічне відставання, обмежений доступ до інновацій
Конкурентні	Стратегічна, ринкова	Агресивна цінова політика конкурентів, демпінг
Кіберзагрози	Інформаційна	Атаки на IT-інфраструктуру, витік конфіденційних даних
Внутрішні загрози		
Фінансові	Фінансова	Неспроможність виконувати зобов'язання, помилки у фінансовому плануванні
Кадрові	Людські ресурси	Плинність кадрів, низький рівень кваліфікації, саботаж
Організаційні	Управлінська	Неефективна структура управління, слабкий контроль
Інформаційні	Інформаційна	Низький рівень захисту даних, внутрішні витоки інформації
Екологічні	Виробнича, репутаційна	Забруднення довкілля, порушення екологічних норм

Джерело: узагальнено на основі [3; 4, с. 236]

Враховуючи численні потенційні загрози, які виникають як всередині підприємств, так і поза ними, організаціям потрібні ефективні механізми для своєчасного виявлення, оцінки та усунення цих ризиків. Сучасне бізнес-середовище, що відзначається швидкоплинністю, непередбачуваністю змін та надлишком інформації, вимагає впровадження принципово нових підходів до забезпечення економічної безпеки. Традиційні методи ризик-аналізу та

прогнозування дедалі частіше виявляються недостатніми у складних умовах сучасної інформаційної екосистеми.

Для ефективного використання інформаційного потенціалу, підприємству необхідно регулярно збирати, структурувати та аналітично обробляти великі обсяги даних. Реалізація цього процесу забезпечується цифровою трансформацією бізнесу через інтеграцію сучасних технологій у всі аспекти діяльності організації. Інноваційні технології відіграють ключову роль у зміцненні економічної безпеки, оскільки сприяють зниженню ризиків, підвищенню операційної ефективності, забезпеченню фінансової стабільності та посиленню конкурентоспроможності підприємства.

Одним із важливих напрямів цифрової трансформації підприємств, що безпосередньо впливає на їх економічну безпеку, є впровадження інструментів штучного інтелекту. Зокрема, розвиток інтерпретованого штучного інтелекту (Explainable AI) відкриває можливості для прозорого та контрольованого прийняття управлінських рішень у складних нейронних мережах. Це особливо важливо з огляду на формування довіри до технологій, дотримання регуляторних вимог та запобігання внутрішнім загрозам, які можуть виникати через непрозорість алгоритмів («чорні скриньки») [11].

Водночас цифрова трансформація змінює підходи до організації фінансової діяльності. Сучасні підприємства дедалі частіше інтегрують елементи децентралізованих фінансів (DeFi), які, попри інноваційність, несуть певні загрози через недостатню регуляцію. У зв’язку з цим, як зазначається в актуальних європейських дослідженнях, впровадження правових механізмів нагляду за DeFi-платформами сприяє забезпеченню фінансової прозорості, зниженню ризику шахрайства та узгодженості з принципами економічної безпеки [12].

Ще одним цифровим інструментом, що сприяє зниженню фінансових ризиків та формуванню стійких бізнес-моделей, є стратегія MVP (Minimum Viable Product). Її застосування дозволяє тестувати бізнес-гіпотези в умовах

ISSN: 2786-9431

обмежених ресурсів, використовуючи хмарні платформи, цифрові середовища та системи швидкого прототипування. Це, у свою чергу, підвищує гнучкість та адаптивність підприємств до мінливих ринкових умов і зменшує ймовірність економічних втрат у разі невдалих рішень [13].

Поряд із цим, в умовах цифровізації фінансового середовища, актуалізується потреба у належному правовому регулюванні новітніх активів, зокрема, криптовалют. Визначення їх правового статусу, особливо у випадках поділу майна або здійснення фінансових операцій, має безпосередній вплив на юридичну безпеку підприємств, а відтак і на загальний рівень їх економічної безпеки [14].

Особливої актуальності у контексті модернізації підприємств за останні роки набули технології великих даних [6] та прогнозної аналітики [9], які дозволяють підприємствам збирати та обробляти великі обсяги даних у режимі реального часу, передбачати ринкові тенденції, ідентифікувати потенційні фінансові та операційні ризики, а також адаптувати бізнес-пропозиції відповідно до потреб клієнтів та прогнозувати їх поведінку і приймати стратегічно важливі управлінські рішення [5, с. 33].

Впровадження аналітики великих даних відкриває нові можливості для оперативного виявлення проблем у фінансових потоках, контролю витрат і оптимізації розподілу ресурсів. Окрім того, штучний інтелект, інтегрований у ці системи, здатен аналізувати клієнтську поведінку, що сприяє більш ефективній адаптації маркетингових стратегій і підвищенню конкурентоспроможності підприємств [8, с. 226].

В умовах сучасних українських реалій особлива актуальність використання технологій великих даних зумовлена низкою ключових факторів.

1. Високий рівень кіберзагроз, зокрема, хакерських атак на підприємства критичної інфраструктури.

ISSN: 2786-9431

Зростання цифрової трансформації бізнесу відкриває нові можливості, але водночас збільшує ризики втручання зловмисників в інформаційні системи підприємств. Кібератаки можуть призводити до втрати конфіденційних даних, фінансових збитків, порушення операційної діяльності та значного зниження довіри клієнтів і партнерів.

Враховуючи важливість захисту підприємств від кіберзагроз, доцільно систематизувати їх основні види, які становлять найбільшу небезпеку для бізнесу на мікрорівні (табл.3).

Таблиця 3

Кіберзагрози, які становлять найбільшу небезпеку для бізнесу в Україні

Кіберзагроза	Опис та наслідки
Фішинг	Один із найпоширеніших видів кіберзлочинності, що призводить до значних фінансових втрат. Мета – викрасти конфіденційні дані (облікові записи, дані кредитних карток) шляхом обману користувачів та змусити їх встановити шкідливе програмне забезпечення. 91% кібератак починаються з фішингового електронного листа
Шкідливе програмне забезпечення	Використовується для встановлення бекдор-доступу до пристроїв компанії, що дає змогу хакерам дистанційно керувати системами, красти дані, досліджувати мережу або розсилати спам. Тісно пов'язане з фішингом
Програми-вимагачі (ransomware)	Блокують інформаційні системи підприємства, позбавляючи доступу до важливих даних, доки не буде сплачено викуп. Часто бізнес змушений платити, але навіть у цьому випадку немає гарантії повернення доступу
Компрометація корпоративної пошти (BEC)	Злочинці отримують доступ до платіжних систем і вводять в оману співробітників, змушуючи їх переказувати кошти на фальшиві рахунки. Ці шахрайства складно виявити і вони призводять до значних фінансових втрат
Внутрішні загрози	Недобросовісні чи незадоволені співробітники, партнери чи підрядники можуть поширювати конфіденційну інформацію або навмисно завдавати шкоди. Внутрішні загрози спричиняють приблизно 25% усіх порушень безпеки
Ненавмисне розголошення	Помилки співробітників (наприклад, випадкове надсилання листів не тим адресатам) можуть призвести до витоку важливої інформації і фінансових збитків, особливо у великих компаніях з великою кількістю персоналу
Інтелект сховища (cloud storage risks)	Незахищені хмарні сховища стають легкою здобиччю для кіберзлочинців. Наприклад, відоме порушення безпеки S3-хмарного сховища Агентства національної безпеки США у 2017 році. Компанії повинні впроваджувати адекватні заходи захисту для збереження конфіденційної інформації в хмарі

Соціальна інженерія	Використання підроблених профілів у соцмережах та інших формах маніпуляції для завоювання довіри жертв і отримання конфіденційної інформації. Цей метод допомагає реалізувати фішинг і поширення шкідливого ПЗ для досягнення фінансової вигоди

Джерело: узагальнено на основі [7; 15]

Таким чином, в умовах підвищеного кіберризику, своєчасне виявлення та аналіз загроз за допомогою технологій великих даних стає критично важливим інструментом для економічної безпеки підприємств.

Аналітика великих даних також дозволяє підвищити рівень захисту бізнес-процесів від внутрішніх загроз, зокрема, шляхом виявлення аномальної поведінки співробітників або підрядників, що може свідчити про потенційний витік даних чи інсайдерські дії.

2. Економічна турбулентність, пов'язана з війною, зовнішньоекономічними викликами, змінами податкового середовища.

В умовах повномасштабної війни та глобальної економічної нестабільності українські підприємства функціонують у середовищі високої волатильності, що ускладнює прийняття стратегічних рішень. Використання великих даних дозволяє підприємствам вчасно і точно прогнозувати наслідки макроекономічних змін, спираючись на великі масиви даних з різних джерел, зокрема:

– моделювати вплив валютних коливань. Це передбачає аналіз змін обмінних курсів та прогнозування їх впливу на цінову політику, експортно-імпортні операції, логістичні процеси та закупівлю сировини. Наприклад, підприємства можуть оптимізувати графіки закупівель або укладати контракти, з урахуванням прогнозованих валютних трендів;

– моніторити податкове та митне середовище. Аналітика великих даних дозволяє оперативно відстежувати зміни у законодавстві, ставки податків, пільги чи обмеження, моделюючи їх вплив на фінансову діяльність компанії. Це забезпечує готовність до змін і мінімізацію податкових ризиків;

– оцінювати геополітичні ризики та динаміку зовнішньоекономічних процесів. Збір даних з новин, звітів міжнародних організацій, соціальних мереж та аналітичних платформ, дозволяє прогнозувати ризики ведення бізнесу в окремих країнах чи регіонах, а також оцінювати ймовірність порушення ланцюгів постачання;

– прогнозувати інфляційні процеси. Аналіз масивів даних щодо динаміки цін на енергоносії, транспортні послуги, продовольство тощо допомагає оцінювати інфляційні загрози, формувати стратегії ціноутворення та бюджетування.

Показовим є кейс використання великих даних для моніторингу постачання скрапленого природного газу в умовах російсько-української війни. Так, у відповідь на збройну агресію росії проти України, значно змінилася географія світового постачання газу. Для аналізу цих змін застосовано масиви великих даних, отриманих із автоматичної ідентифікаційної системи суден (AIS), що фіксує траєкторії руху морського транспорту у реальному часі [16]. Завдяки такому підходу стало можливим оперативно відстежувати логістичні ланцюги, вчасно реагувати на потенційні перебої та мінімізувати ризики, пов’язані з порушеннями постачання, що істотно підвищує рівень енергетичної стабільності.

Отже, використання великих даних в умовах економічної турбулентності – це не лише інструмент аналізу, а й необхідний елемент забезпечення економічної безпеки підприємств.

3. Потреба у підвищенні прозорості та зниженні рівня корупційних ризиків.

Українські підприємства сьогодні працюють у надзвичайно складному економічному середовищі, яке характеризується високою невизначеністю та ризиками, що значно ускладнює процес прийняття стратегічних рішень. Використання великих даних дозволяє виявляти складні фінансові моделі, полегшує виявлення аномалій та покращує прогностичні можливості

правоохоронних органів. Обробляючи величезні обсяги даних, включаючи фінансові транзакції та записи комунікацій, аналітика великих даних виявляє приховані зв'язки та системні порушення, які традиційні методи можуть пропустити [17, с. 138].

Таким чином, великі дані забезпечують динамічне управління ризиками, дозволяючи адаптувати бізнес-модель до нових умов і прогнозувати загрози, перш ніж вони стануть критичними.

Отже, у світі, що стрімко змінюється, великі дані стають фундаментальним інструментом для сучасного бізнесу, особливо в умовах підвищеної невизначеності та ризиків. Завдяки своїй здатності інтегрувати різноманітні джерела інформації та забезпечувати їх глибокий аналіз, вони відкривають нові горизонти для розуміння складних процесів і прийняття більш ефективних рішень. Використання великих даних трансформує традиційні підходи до управління ризиками та безпекою, роблячи акцент на превентивних заходах і адаптивності підприємств.

Висновки. Отже, роль великих даних у прогнозуванні загроз економічної безпеки підприємств в Україні є надзвичайно важливою, оскільки вони дозволяють виявляти потенційні ризики ще на етапі їх формування. Систематичне збирання, обробка та аналіз інформаційних потоків створює умови для більш точного передбачення фінансових, операційних та кіберзагроз. Завдяки впровадженню інструментів великих даних підприємства можуть оперативно реагувати на зміну зовнішнього середовища та уникати критичних втрат. Аналітика на основі великих даних сприяє прийняттю обґрунтованих управлінських рішень, що підвищує загальну стійкість бізнесу. Особливо актуальним це є для українських підприємств в умовах високої турбулентності ринку, воєнних дій та економічної нестабільності. Впровадження цифрових технологій створює нові перспективи для формування ефективної системи управління ризиками. Тому технології

ISSN: 2786-9431

великих даних є не лише засобом підвищення операційної ефективності, а й важливим фактором забезпечення економічної безпеки підприємств.

Список використаних джерел

1. Петренко Л. М., Худіков П. В. Економічна безпека підприємства: фактори та загрози. *Наукові інновації та передові технології*. 2024. № 12(40). С. 788–798. DOI: https://doi.org/10.52058/2786-5274-2024-12(40)-788-798.

2. Васюткіна Н., Ватащук В. Фактори впливу на формування системи економічної безпеки підприємства в умовах динамічності конкурентного середовища. *Економіка та суспільство*. 2024. № 68. DOI: https://doi.org/10.32782/2524-0072/2024-68-39.

3. Крилов Д. В. Характеристика загроз економічній безпеці підприємства в сучасних умовах. *Проблеми сучасних трансформацій. Серія: економіка та управління.* 2024. № 13. DOI: https://doi.org/10.54929/2786-5738-2024-13-04-07.

4. Popelo O., Shaposhnykov K., Popelo O., Hrubliak O., Malysh V., Lysenko Zh. The influence of digitalization on the innovative strategy of the industrial enterprises development in the context of ensuring economic security. *International Journal of Safety and Security Engineering*. 2023. Vol. 13, № 1. P. 39–49. DOI: https://doi.org/10.18280/ijsse.130105.

5. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету. Економічні науки*. 2020. № 4(1). С. 32–35. URL: http://nbuv.gov.ua/UJRN/Vchnu_ekon_2020_4(1)__7 (дата звернення: 14.04.2025).

6. Вовк О., Стець О., Лазаренко І. Особливості застосування інформаційно-аналітичних технологій Big Data в умовах цифрової економіки. *Підприємництво та інновації.* 2024. Вип. 33. С. 7–12. DOI: https://doi.org/10.32782/2415-3583/33.1.

7. Onyshchenko S., Bilko S., Yanko A., Sivitska S. Business information security. Proceedings of the 4th international conference on building innovations. Lecture notes in civil engineering / eds. V. Onyshchenko, G. Mammadova, S. Sivitska, A. Gasimov. Springer, Cham. 2023. Vol. 299. https://doi.org/10.1007/978-3-031-17385-1_65.

8. Остапчук О., Баксалова О. Інноваційні технології управління в забезпеченні економічної безпеки: мотиваційні аспекти. *Modeling the development of the economic systems.* 2025. № 1. P. 225–231. URL: https://elar.khmnu.edu.ua/handle/123456789/18262 (дата звернення: 13.06.2025).

9. Олійничук О. І. Технологія діяльності аналітиків із питань економічної безпеки підприємства. *Економіка та управління підприємствами*. 2020. Вип 39. С. 201–206. DOI: https://doi.org/10.32843/infrastruct39-33.

10. Лєзіна А. Генеза розвитку дефініції «економічна безпека підприємства». *Сталий розвиток економіки*. 2024. № 2(49). С. 101–106. DOI: https://doi.org/10.32782/2308-1988/2024-49-16.

11. Korostin O. O. Explainable AI: new approaches to interpretability of deep neural networks. Вісник ХНТУ. 2025. № 1(92), Ч. 2. С. 100–106. DOI: https://doi.org/10.35546/kntu2078-4481.2025.1.2.14.

12. Chmielarz P. Regulacja zdecentralizowanych finansów (DeFi) w Unii Europejskiej : wyzwania prawne i nowe mechanizmy nadzoru finansowego w kontekście prawa administracyjnego i finansowego. *Теоретичні та практичні проблеми реалізації норм права* : матеріали X міжнард. наук.-практ. конф. (м. Кременчук, 5-7 грудня 2024 р.). Львів. Торунь: Liha-Pres, 2024. С. 188–191. DOI: https://doi.org/10.36059/978-966-397-452-1-49.

13. Mikadze S. MVP strategy as a tool for business model validation in the early stages of a startup lifecycle. *Актуальні питання економічних наук*. 2024. №6. DOI: https://doi.org/10.5281/zenodo.15484546.

14. Chmielarz P. Bitcoin versus podział majątku wspólnego. *HOMO POLITICUS: ROCZNIK POLITOLOGICZNY*. 2020. № 14(1). P. 43–57. DOI: https://doi.org/10.25312/2391-5110.14/2019_04pch.

15. Borenkov A. TOP 10 Cybersecurity threats to businesses in 2023. BDO Ukraine: website. 2023. URL: https://www.bdo.ua/en-gb/insights-1/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023 (дата звернення: 14.04.2025).

16. Xiao R., Zhao P., Zhang M., Kang T., Ma T. Discovering changes in the global liquefied natural gas marine supply network during the Russian-Ukrainian crisis with Big Data. *Chin. Geogr. Sci.* 35, 295–310 (2025). DOI: https://doi.org/10.1007/s11769-024-1467-0.

17. Chystiakova A., Podliehaiev K., Khoronovskyi O., Sokur T., Kubariev I. The role of big data analytics in the investigation of corruption offences. *Revista Jurídica Portucalense.* 2025. № 37. P. 116–143. DOI: https://doi.org/10.34625/issn.2183-2705(37)2025.ic-6.

18. Horbenko, Y. AI-Powered UI adaptation and data Automation in secure Front-End Systems. *International Journal of Development Research.* 2025. 15, (05), 68383-68388. https://journalijdr.com/ai-powered-ui-adaptation-and-data-automation-secure-front-end-systems