УДК 338.2
JEL: D23; G32; G39; L86
DOI: https://doi.org/10.32983/2222-4459-2024-9-123-129

УДОСКОНАЛЕННЯ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ВІД РИЗИКІВ ШАХРАЙСТВА

©2024 ОДНОШЕВНА О. О., ВІТЕР В. А., КАЛМИКОВ С. О.

УДК 338.2
JEL: D23; G32; G39; L86

Одношевна О. О., Вітер В. А., Калмиков С. О. Удосконалення процесу забезпечення захисту фінансово-економічної безпеки підприємства від ризиків шахрайства

Метою дослідження є вдосконалення методів захисту фінансово-економічної безпеки підприємств від ризиків шахрайства через використання сучасних технологій, таких як штучний інтелект, машинне навчання та блокчейн, а також розвиток організаційних підходів до внутрішнього контролю. У процесі дослідження використано теоретичні та практичні матеріали з питань фінансово-економічної безпеки, нормативно-правові акти, наукові праці вітчизняних і зарубіжних авторів. Методи включають теоретичне узагальнення, аналіз і синтез для розробки підходів до виявлення шахрайства, а також формалізацію для побудови моделі захисту підприємств від шахрайських дій. У статті розроблено концепцію вдосконалення системи захисту підприємств від шахрайства шляхом упровадження сучасних технологічних рішень, таких як автоматизація процесів контролю за допомогою штучного інтелекту, блокчейн-технологій та машинного навчання. Запропоновано підходи до підвищення ефективності внутрішнього контролю, який включає аналіз поведінкових моделей співпрацівників і контрагентів. Система автоматизованого моніторингу дозволяє оперативно виявляти шахрайські дії та мінімізувати втрати підприємств. Подальші дослідження будуть зосереджені на вдосконаленні механізмів інтеграції автоматизованих систем захисту з внутрішніми бізнес-процесами, а також на розробці рекомендацій щодо підвищення корпоративної етики та відповідальності. Це дозволить підприємствам ефективніше протидіяти шахрайству та забезпечити стабільний розвиток в умовах глобалізації.
Ключові слова: *підприємство, фінансово-економічна безпека, шахрайство, внутрішній контроль, штучний інтелект, блокчейн, автоматизація, ризики.*
Рис.: *1.* ***Бібл.:*** *9.*

Одношевна Ольга Олександрівна *– кандидат економічних наук, доцент кафедри обліку, оподаткування та управління фінансово-економічною безпекою, Дніпровський державний аграрно-економічний університет (вул. Академіка Сергія Єфремова, 25, Дніпро, 49027, Україна)*
E-mail: *lelic2602@ukr.net*
ORCID: *https://orcid.org/0000-0002-2670-7659*
Researcher ID: *https://www.webofscience.com/wos/author/record/HNS-8503-2023*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=59180518800*

Вітер Віталій Андрійович *– магістр кафедри обліку, оподаткування та управління фінансово-економічною безпекою, Дніпровський державний аграрно-економічний університет (вул. Академіка Сергія Єфремова, 25, Дніпро, 49027, Україна)*
E-mail: *viterfirs@gmail.com*
ORCID: *https://orcid.org/0009-0008-3164-1368*

Калмиков Сергій Олександрович *– магістр кафедри обліку, оподаткування та управління фінансово-економічною безпекою, Дніпровський державний аграрно-економічний університет (вул. Академіка Сергія Єфремова, 25, Дніпро, 49027, Україна)*
E-mail: *sfinase@gmail.com*

UDC 338.2
JEL: D23; G32; G39; L86

Odnoshevna O. O., Viter V. A., Kalmykov S. O. Improvement of the Process of Ensuring Protection of the Enterprise's Financial and Economic Security from Fraud Risks

The aim of the study is to improve methods of protecting the financial and economic security of enterprises from fraud risks through the use of modern technologies, such as artificial intelligence, machine learning and blockchain, as well as the development of organizational approaches to internal control. In the course of the study, theoretical and practical materials on financial and economic security, normative legal acts, scientific works of domestic and foreign authors were used. The methods include theoretical generalization, analysis and synthesis to develop approaches to fraud detection, as well as method of formalization to build a model for protecting enterprises from fraudulent activities. The article develops a conception for improving the system of protection of enterprises from fraud through the introduction of modern technological solutions, such as automation of control processes using artificial intelligence, blockchain technologies and machine learning. Approaches to improving the efficiency of internal control, which includes the analysis of behavioral models of employees and contractors, have been proposed. E. g., the automated monitoring system allows you to quickly detect fraudulent activities and minimize the losses of enterprises. Further research will focus on improving the mechanisms for integrating automated security systems with internal business processes, also on developing recommendations for improving corporate ethics and responsibility. This will allow enterprises to counteract fraud more effectively and ensure stable development in the context of globalization.
Keywords: *enterprise, financial and economic security, fraud, internal control, artificial intelligence, blockchain, automation, risks.*
Fig.: *1.* ***Bibl.:*** *9.*

Odnoshevna Olha O. *– PhD (Economics), Associate Professor of the Department of Accountancy, Taxation and Management of Financial and Economic Security, Dnipro State Agrarian and Economic University (25 Academika Serhiia Yefremova Str., Dnipro, 49027, Ukraine)*
E-mail: *lelic2602@ukr.net*
ORCID: *https://orcid.org/0000-0002-2670-7659*
Researcher ID: *https://www.webofscience.com/wos/author/record/HNS-8503-2023*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=59180518800*

Viter Vitalii A. *– Master of the Department of Accountancy, Taxation and Management of Financial and Economic Security, Dnipro State Agrarian and Economic University (25 Academika Serhiia Yefremova Str., Dnipro, 49027, Ukraine)*
E-mail: *viterfirs@gmail.com*
ORCID: *https://orcid.org/0009-0008-3164-1368*
Kalmykov Sergiy O. *– Master of the Department of Accountancy, Taxation and Management of Financial and Economic Security, Dnipro State Agrarian and Economic University (25 Academika Serhiia Yefremova Str., Dnipro, 49027, Ukraine)*
E-mail: *sfinase@gmail.com*

Стрімка цифровізація та глобалізація бізнес-середовища суттєво підвищують ризики шахрайства у фінансово-економічній сфері. Зокрема, складність ринкових відносин і широке використання інформаційних технологій створюють нові можливості для зловмисників. Традиційні методи захисту втрачають ефективність, що вимагає вдосконалення підходів до захисту фінансово-економічної безпеки підприємств. Це питання стає критично важливим у контексті управління ресурсами, стратегії розвитку та конкурентоспроможності.

У сучасних дослідженнях з фінансового менеджменту та фінансово-економічної безпеки підприємств значний внесок зробили як вітчизняні, так і зарубіжні дослідники. Зокрема, Г. О. Партин та Н. Є. Селюченко [4] висвітлюють комплексні підходи до управління фінансовими ресурсами підприємства, включно з управлінням прибутком, активами та ризиками. Автори зосереджуються на механізмах антикризового фінансового управління, що є важливим аспектом в умовах сучасних викликів для підприємств.

У підручнику [2] розглядаються основні принципи організації фінансів підприємств, включно з управлінням активами та оподаткуванням. Окрему увагу приділено показникам фінансового стану підприємств і фінансовій санації, що дозволяє зрозуміти важливі аспекти фінансової стійкості бізнесу.

Бондарчук М. К. та Алєксєєва І. В. [1] акцентують увагу на механізмах санації підприємств та антикризовому управлінні, що є ключовими елементами для забезпечення фінансової стійкості підприємств в умовах кризи.

О. В. Сусіденко у монографії [5] досліджує різні підходи до забезпечення фінансової безпеки на підприємствах, особливо під час управління ризиками, що пов'язані з шахрайством та іншими загрозами. Праця охоплює теоретичні та практичні аспекти, що робить її корисною для широкого кола спеціалістів.

J. T. Wells [9] надає практичні рекомендації щодо запобігання шахрайству на корпоративному рівні, пропонуючи інструменти для ефективної боротьби з цими загрозами.

Важливу роль у побудові стратегії управління ризиками відіграє праця C. L. Pritchard [8], де акцентується на процесах управління ризиками в контексті захисту фінансової безпеки підприємств.

Не можна оминути увагою і дослідження Остапова С. Є. зі співавторами [3], де розглядаються сучасні методи шифрування та захисту інформації, що має значення для запобігання кіберзлочинам, зокрема фішинговим атакам, які становлять загрозу фінансовій стабільності підприємств.

У сучасних умовах стрімкої цифровізації та глобалізації бізнес-середовища питання захисту фінансово-економічної безпеки підприємств набуває дедалі більшої ваги. Зростаюча складність ринкових відносин, розширення використання цифрових технологій, а також інтеграція бізнес-процесів на міжнародному рівні створюють нові можливості для шахрайських дій. Ці явища значно ускладнюють контроль за рухом фінансових потоків та безпекою інформації, що ставить під загрозу стабільність функціонування підприємств. Ба більше, зловмисники активно використовують нові технологічні інструменти для обходу традиційних механізмів захисту, що ускладнює виявлення шахрайських схем і мінімізує ефективність запобіжних заходів.

Проблема шахрайства полягає не лише у прямих фінансових збитках, але й у довготривалих негативних наслідках для підприємства. Шахрайські дії можуть призвести до значного зниження репутаційного капіталу, підриву довіри з боку партнерів, інвесторів та клієнтів, що є особливо небезпечним у сучасних умовах конкуренції. Ризики шахрайства впливають на всі аспекти діяльності підприємства, включно з управлінням ресурсами, стратегією розвитку та інвестиційними рішеннями. Порушення довіри до фінансової прозорості та надійності компанії може мати катастрофічні наслідки для її довгострокової конкурентоспроможності та навіть призвести до банкрутства.

У зв'язку з цим питання вдосконалення процесу захисту від шахрайства повинно бути розглянуто як стратегічне завдання, що вимагає комплексного підходу. Це включає не лише технологічні інструменти та засоби контролю, але й формування культури корпоративної відповідальності та прозорості. Успішне запобігання шахрайству залежить

від здатності підприємства адаптуватися до нових загроз і вчасно реагувати на зміни в ризиковому середовищі. Важливою складовою цього процесу є також прогнозування шахрайських ризиків та створення надійних моделей раннього попередження.

Особливу увагу слід приділити шахрайству, яке виникає зсередини компанії. Внутрішні загрози часто важко виявити через довіру до персоналу та доступ співробітників до критично важливої інформації. Таким чином, ефективні методи управління внутрішніми ризиками, що включають регулярний аудит, підвищення обізнаності співробітників щодо етичних стандартів, а також посилення контролю за доступом до фінансових ресурсів, повинні стати важливим елементом стратегії захисту. Це забезпечить комплексний підхід до мінімізації шахрайства та сприятиме підвищенню загальної стійкості підприємства.

Метою даної статті є всебічне дослідження та вдосконалення методів захисту фінансово-економічної безпеки підприємств від ризиків шахрайства. Основне завдання полягає в пошуку та розробці ефективних інструментів, які дозволять не лише виявляти шахрайські дії на ранніх стадіях, але й запобігати їм.

Для досягнення цієї мети необхідно вдосконалити методи внутрішнього контролю, які відіграють ключову роль у забезпеченні фінансової стабільності та зниженні ризиків шахрайства. Традиційні системи внутрішнього контролю, засновані на ручних перевірках та аудитах, втрачають свою ефективність у зв'язку зі збільшенням обсягів фінансових операцій та складністю шахрайських схем. У зв'язку з цим важливо дослідити можливості автоматизації процесів контролю та використання аналітичних інструментів для виявлення відхилень у фінансових даних.

Одним із ключових напрямків дослідження є використання сучасних інструментів аналізу даних, таких як штучний інтелект, машинне навчання та блокчейн-технології. Ці інструменти дозволяють не лише аналізувати великі масиви даних у реальному часі, але й ідентифікувати приховані закономірності, які можуть свідчити про потенційне шахрайство. Наприклад, системи машинного навчання здатні самостійно вивчати поведінкові моделі та визначати підозрілі транзакції або дії, що відрізняються від звичайних операцій.

Також важливо розглянути питання організаційної культури та обізнаності співробітників щодо ризиків шахрайства. Формування етичної поведінки, постійне навчання персоналу та розробка внутрішніх політик, спрямованих на запобігання шахрайським діям, можуть значно знизити ймовірність внутрішніх загроз. Створення системи відповідальності та прозорості у взаємодії між співробітниками допоможе зменшити рівень шахрайства зсередини.

Таким чином, *завданням* даної статті є розробка комплексного підходу до захисту підприємств від шахрайства, який поєднує сучасні технологічні рішення з організаційними заходами та внутрішнім контролем. Це дозволить не лише підвищити ефективність боротьби з шахрайством, але й мінімізувати його негативний вплив на фінансово-економічну безпеку підприємств у довгостроковій перспективі.

Дослідження виконувалося у кілька етапів.

1. Теоретичний етап

Першим етапом дослідження стало глибоке вивчення наукових праць та публікацій, присвячених питанням забезпечення фінансово-економічної безпеки підприємств, особливо в контексті боротьби з шахрайством. Було проведено аналіз таких праць: Сусіденко О. В. [5], де висвітлено різні аспекти управління ризиками на підприємствах, включно з методами захисту від шахрайства. Окрім того, важливу інформацію було взято з праці Дж. Т. Веллса [9], яка пропонує практичні рекомендації для боротьби з корпоративним шахрайством, що є ключовим у даному дослідженні.

На цьому етапі особливу увагу було приділено також аналізу сучасних інструментів кіберзахисту, таких як шифрування та блокчейн-технології, описані в роботі Остапова С. Є., Євсеєва С. П., Король О. Г. [3]. Це дозволило створити теоретичне підґрунтя для формулювання напрямів подальших досліджень та впровадження новітніх технологій у боротьбу з шахрайськими схемами.

2. Аналіз сучасних технологій захисту

Другим етапом було вивчення сучасних технологічних рішень, які можуть бути використані для підвищення захисту фінансових даних підприємств. Основна увага приділялася інструментам автоматизації процесів контролю, що включають використання штучного інтелекту, машинного навчання та блокчейн-технологій для виявлення шахрайства в реальному часі. Наприклад, у дослідженні Партин Г. О. та Селюченко Н. Є. [4] було висвітлено механізми антикризового управління фінансовими ресурсами, що надало основу для розробки систем моніторингу та контролю фінансових транзакцій. Застосування алгоритмів машинного навчання для аналізу великих масивів даних дозволяє автоматично виявляти підозрілі фінансові операції та поведінкові відхилення, що може свідчити про шахрайські дії. Використання блокчейн-технологій у цьому процесі дозволяє за-

безпечити прозорість і незмінність даних, що значно знижує ризики підробки інформації.

3. Практичний етап – моделювання захисту

На третьому етапі було розроблено модель комплексного підходу до захисту фінансово-економічної безпеки підприємств. Основна увага зосереджувалася на впровадженні систем автоматизованого моніторингу й аналізу електронної пошти для виявлення фішингових атак. Було запропоновано інтеграцію інструментів для аналізу поведінки користувачів та алгоритмів машинного навчання, що дозволить виявляти нові, ще не відомі загрози.

Згідно з рекомендаціями, наведеними у дослідженнях Дж. Т. Веллса [9] та К. Л. Прітчарда [8], особливу увагу було приділено управлінню ризиками на корпоративному рівні та побудові системи внутрішнього контролю. Практичне використання цих інструментів на підприємствах дозволяє знижувати ризики шахрайських дій і підвищувати загальну безпеку фінансових операцій.

4. Емпіричний етап – оцінка результатів

На завершальному етапі було проведено емпіричне дослідження для оцінки ефективності розроблених методів. Системи автоматичного моніторингу фішингових атак були протестовані на вибраних підприємствах, які активно працюють у сфері аутсорсингу. Аналіз результатів показав, що використання сучасних технологічних рішень дозволяє значно знизити кількість шахрайських випадків. Зокрема, було встановлено, що автоматизація процесів контролю та використання блокчейн-технологій підвищують надійність фінансових операцій і забезпечують додатковий рівень захисту даних.

Фішингові атаки є одним із найбільш поширених способів шахрайства, що використовуються для отримання доступу до конфіденційної інформації компаній. Особливо вразливими є аутсорсингові компанії, які зазвичай мають широкий доступ до інформації клієнтів і проводять транзакції від їхнього імені [6]. Це створює додаткові можливості для шахраїв, які можуть використовувати фальшиві запити для отримання доступу до фінансових та інших конфіденційних даних.

Пропоноване програмне забезпечення має на меті запобігання таким атакам шляхом постійного автоматичного моніторингу електронної пошти співробітників, які відповідають за виконання фінансових операцій. Воно буде інтегроване з корпоративною поштовою системою й автоматично перевірятиме вхідні повідомлення на наявність ознак фішингової діяльності. Ці ознаки можуть включати зміни в структурі листа, відхилення від стандартних запитів клієнта або будь-які інші підозрілі дії, що можуть вказувати на спроби шахрайства. При виявленні такої діяльності особа, яка працює з цим клієнтом, буде завчасно попереджена, що саме цей отриманий запит передбачає потенційно небезпечні дії. У такому випадку виконавець вже буде мати розуміння, що йому потрібно більш детально перевірити мету цього повідомлення та за потреби додатково зв'язатися з клієнтом для з'ясування достовірності попередньо отриманого листа.

Особливістю цього підходу є можливість створення адаптивної системи на основі машинного навчання. Система буде здатна «навчатися» на основі вже відомих випадків фішингових атак, що дозволить їй виявляти нові, ще невідомі загрози. За допомогою алгоритмів аналізу поведінкових клієнтів і шахраїв програмне забезпечення буде виявляти та попереджати про потенційно небезпечні запити. Це знизить ризики автоматичного виконання операцій, що могли бути спричинені фішинговими атаками.

ІННОВАЦІЙНА КОНЦЕПЦІЯ ГІБРИДНОГО ШИФРУВАННЯ

Удосконалення технології шифрування є ключовим для забезпечення ще більш високого рівня захисту. У даному дослідженні пропонується новий підхід до гібридного шифрування, який включає поєднання гомоморфного та асиметричного шифрування для забезпечення конфіденційності на всіх етапах обробки даних.

Основна інновація полягає в тому, що запропоноване рішення дозволяє обробляти дані без необхідності їх розшифрування, що мінімізує ризики витоку інформації під час виконання обчислень. За допомогою гомоморфного шифрування можна виконувати операції над зашифрованими даними, що робить процеси більш безпечними й ефективними.

Асиметричне шифрування додає додатковий рівень захисту під час передачі симетричних ключів, що використовуються для основного шифрування даних. Кожен ключ передається зашифрованим за допомогою RSA або ECC, що робить процес передачі ключів захищеним від несанкціонованого доступу [7].

Запропоноване рішення відкриває нові перспективи для подальшого вдосконалення інформаційних систем, дозволяючи ефективніше захищати фінансово-економічну безпеку підприємств.

Послідовність роботи концепції програмного забезпечення

1. Інтеграція з електронною поштою компанії:

- Програмне забезпечення підключається до поштових серверів компанії та отримує доступ до всіх поштових скриньок співробіт-

ників, які мають потенційний ризик отримання фішингових повідомлень.

- Система автоматично визначає користувачів, які регулярно взаємодіють з клієнтами або здійснюють фінансові операції.

2. Аналіз вхідних повідомлень:

- Після отримання нового електронного листа програмне забезпечення негайно починає аналіз його змісту.
- Для цього використовується база даних ознак фішингових атак, яка містить відомі шаблони шахрайських повідомлень (несподівані зміни в інструкціях, вимоги термінових операцій, зміни в рахунках або даних отримувача платежів тощо).
- Також система перевіряє відправника листа, використовуючи алгоритми для виявлення підроблених адрес або зламаних поштових акаунтів клієнтів.

3. Поведінковий аналіз та навчання:

- Паралельно з аналізом вмісту повідомлень система проводить поведінковий аналіз. Вона вивчає, як зазвичай клієнт поводиться в комунікації (що запитує, які дії зазвичай виконує).
- Використовуючи алгоритми машинного навчання, програмне забезпечення постійно оновлює свою базу шаблонів фішингових атак та адаптується до нових загроз, розпізнаючи невідомі раніше шахрайські патерни.

4. Виявлення підозрілих листів:

- Якщо виявлено аномальні зміни або ознаки фішингової атаки (наприклад, термінові прохання про зміну фінансових даних або підозрілі посилання), програмне забезпечення автоматично позначає та блокує лист до перевірки.
- Повідомлення надсилається співробітнику або відповідальній особі з попередженням, що в листі можуть бути шахрайські наміри. Пропонується перевірити інформацію додатково.

5. Додаткова перевірка автентичності:

- Співробітник, отримавши попередження, зобов'язаний перевірити запит, зв'язавшись із клієнтом через інший канал зв'язку (наприклад, телефон).
- Якщо клієнт підтверджує, що запит дійсно надійшов від нього, лист розблоковується для подальшого виконання запиту.

6. Автоматичне оновлення бази даних:

- Кожен випадок виявлення шахрайської активності або підтвердження автентичності запиту вноситься до бази даних.
- Програмне забезпечення аналізує ці випадки, вдосконалюючи алгоритми для швидшого та точнішого виявлення майбутніх фішингових атак. Це дозволяє системі адаптуватися до змінюваних методів шахраїв.

7. Захист від витоку інформації через шифрування:

- Усі дані, що проходять через програмне забезпечення, включно з поштовими повідомленнями та інформацією про шахрайські спроби, шифруються за допомогою інноваційного гібридного шифрування.
- Гомоморфне шифрування забезпечує можливість обробки зашифрованих даних без необхідності їх розшифровувати, що мінімізує ризики витоку інформації навіть під час виконання операцій.
- Асиметричне шифрування використовується для передачі ключів між співробітниками або серверами для додаткового рівня захисту.

8. Звітування та аудити:

- Програмне забезпечення формує детальні звіти про всі підозрілі листи, дії співробітників і підтверджені випадки шахрайства.
- Ці звіти можуть бути використані для внутрішнього аудиту безпеки або надання додаткових доказів у разі судових розслідувань.

9. Безперервний моніторинг і поліпшення:

- Система працює в безперервному режимі, здійснюючи моніторинг усіх вхідних повідомлень. Програмне забезпечення регулярно оновлює свої алгоритми на основі нових виявлених фішингових атак і зламаних акаунтів.
- Компанія може додавати нові правила та критерії для виявлення загроз, враховуючи специфіку роботи своїх співробітників та клієнтів.

10. Масштабованість і гнучкість:

- Програмне забезпечення розроблено таким чином, щоби бути масштабованим і гнучким, дозволяючи адаптувати його під потреби як малих, так і великих компаній. Система може працювати з великим обсягом поштових акаунтів та легко інтегруватися з наявними системами управління ризиками та інформаційної безпеки.

Концептуальну схему роботи програмного забезпечення наведено на *рис. 1*.

ВИСНОВКИ

Автоматизація процесу виявлення фішингових атак дозволить значно зменшити кількість випадків шахрайства, пов'язаних з електронною поштою, що є одним із основних каналів здійснення

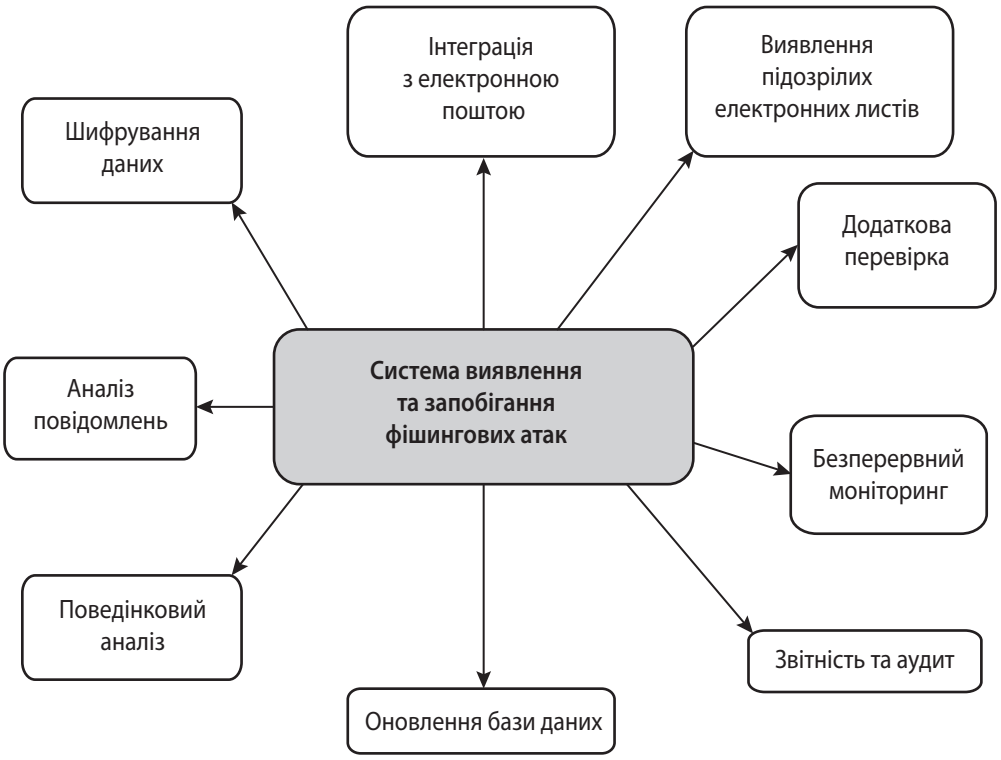

Рис. 1. Схема роботи програмного забезпечення для захисту від фішингових атак

Джерело: авторська розробка.

шахрайських операцій. Використання гомоморфного шифрування під час обробки даних гарантує, що жодна конфіденційна інформація не буде доступною навіть під час її обробки, що суттєво зменшує ризики витоку інформації. Завдяки поєднанню гомоморфного шифрування з асиметричним переданням ключів буде досягнуто максимального рівня безпеки під час як обробки, так і передачі даних.

Це робить дану технологію перспективною для застосування не лише в аутсорсингових компаніях, але й на будь-яких інших підприємствах, що працюють з конфіденційною інформацією.

Окрім цього, впровадження таких технологій допоможе підвищити рівень довіри клієнтів до підприємств, які використовують сучасні методи захисту інформації, та мінімізувати потенційні збитки, що можуть бути спричинені шахрайськими діями. Таким чином, використання запропонованої концепції сприятиме зміцненню фінансово-економічної безпеки підприємств у довгостроковій перспективі. ■

БІБЛІОГРАФІЯ

1. Бондарчук М. К., Алєксєєв І. В. Фінансова санація і антикризове управління підприємством (з перекладом тем англійською мовою) : навч. посіб. Львів : Видавництво Львівської політехніки, 2017. 268 с.
2. Курило О. Б., Бондаренко Л. П., Вівчар О. І., Чубка О. М. Фінанси підприємств : підручник. Київ : ВД «Кондор», 2020. 340 с.
3. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека сучасні технології захисту : навч. посіб. Київ : Новий світ-2000, 2023. 678 с.
4. Партин Г. О., Селюченко Н. Є. Фінансовий менеджмент : підручник. Львів : Видавництво Львівської політехніки, 2018. 388 с.
5. Сусіденко О. В. Фінансова безпека підприємства: теорія, методи, практика. Київ : ЦУЛ, 2019. 128 с.
6. Унінець-Ходаківська В. П., Костюкевич О. І., Лятамбор О. А. Ринок фінансових послуг: теорія і практика. Київ : ЦУЛ, 2021. 392 с.
7. Гончаренко Д. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? *HostPro*. 16.07.2020. URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/
8. Pritchard C. L. Risk Management: Concepts and Guidance. 5th ed. London; New York : CRC Press, 2015. 466 p.
9. Wells J. T. Corporate Fraud Handbook: Prevention and Detection. 5th ed. Hoboken, NJ : Wiley, 2017. 432 p.

REFERENCES

Bondarchuk, M. K., and Alieksieiev, I. V. *Finansova sanatsiia i antykryzove upravlinnia pidpryiemstvom (z perekladom tem anhliiskoiu movoiu)* [Financial Rehabilitation and Anti-crisis Management of the Enter-

prise (with Translation of Topics into English)]. Lviv: Vydavnytstvo Lvivskoi politekhniky, 2017.
Honcharenko, D. "Shyfruvannia: typy i alhorytmy. Shcho tse, chym vidrizniaiutsia i de vykorystovuiutsia?" [Encryption: Types and Algorithms. What Is It, How are They Different and Where are They Used?]. *HostPro*. July 16, 2020. https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/
Kurylo, O. B. et al. *Finansy pidpryiemstv* [Enterprise Finance]. Kyiv: VD «Kondor», 2020.
Ostapov, S. E., Yevseiev, S. P., and Korol, O. H. *Kiberbezpeka suchasni tekhnolohii zakhystu* [Cyber Security Modern Protection Technologies]. Kyiv: Novyi svit-2000, 2023.
Partyn, H. O., and Seliuchenko, N. Ye. *Finansovyi menedzhment* [Financial Management]. Lviv: Vydavnytstvo Lvivskoi politekhniky, 2018.
Pritchard, C. L. *Risk Management: Concepts and Guidance*. London; New York: CRC Press, 2015.
Susidenko, O. V. *Finansova bezpeka pidpryiemstva: teoriia, metody, praktyka* [Financial Security of the Enterprise: Theory, Methods, Practice]. Kyiv: TsUL, 2019.
Uninets-Khodakivska, V. P., Kostiukevych, O. I., and Liatambor, O. A. *Rynok finansovykh posluh: teoriia i praktyka* [Market of Financial Services: Theory and Practice]. Kyiv: TsUL, 2021.
Wells, J. T. *Corporate Fraud Handbook: Prevention and Detection*. Hoboken, NJ: Wiley, 2017.

УДК 330.4:519.8
JEL: C89; D21; F31; L86; O24
DOI: https://doi.org/10.32983/2222-4459-2024-9-129-138

МОДЕЛІ АНАЛІЗУ ДИНАМІКИ РИНКУ КРИПТОВАЛЮТ З УРАХУВАННЯМ ПОВЕДІНКОВИХ МЕТРИК СТЕЙКХОЛДЕРІВ ЗА ДАНИМИ СОЦІАЛЬНИХ МЕРЕЖ

©2024 **ГУР'ЯНОВА Л. С., ЛУЦЕНКО Р. Р.**

УДК 330.4:519.8
JEL: C89; D21; F31; L86; O24

Гур'янова Л. С., Луценко Р. Р. Моделі аналізу динаміки ринку криптовалют з урахуванням поведінкових метрик стейкхолдерів за даними соціальних мереж

Використання методів інтелектуального аналізу даних у контексті поведінкової економіки віртуальних активів на основі даних соціальних мереж дозволяють більш точно оцінювати цінові рухи криптовалют. У дослідженні побудовано моделі прогнозування цін на ринку криптовалют з урахуванням поведінкових факторів стейкхолдерів на основі соціальних даних із платформи TikTok. Дані для цього дослідження отримані за допомогою прикладних програмних інтерфейсів соціальних мереж. Основні етапи дослідження включали збір даних, їх обробку та агрегацію, масштабування та кореляційний аналіз, побудову та оцінку моделей. У результаті дослідження визначено ключові поведінкові метрики соціальних мереж. Кореляційний аналіз продемонстрував наявність сильних лінійних зв'язків між соціальними показниками TikTok та слабкі зв'язки із ціною біткоїна. У дослідженні побудовані лінійні моделі, поліноміальна регресія, дерево рішень та «випадковий ліс». Використані такі поведінкові метрики, як кількість публікацій, лайків, коментарів, поширень і переглядів. Проведено оцінку моделей шляхом тестування за допомогою метрик MSE і MAE. Результати свідчать про обмежену ефективність лінійної регресії для прогнозування цін на криптовалюти через нелінійну природу ринку. Модель дерева рішень продемонструвала певний успіх у прогнозуванні цін на біткоїн, проте зросли відхилення у прогнозах з часом, особливо в умовах ринкових коливань. Поліноміальна регресія і модель «випадкового лісу» демонструють вищу точність у прогнозах. На основі порівняння показників MSE і MAE «випадковий ліс» виявився найефективнішою моделлю для прогнозування цін біткоїна серед розглянутих.

Ключові слова: *криптовалюти, патерни поведінки, API (application programming interface), соціальні мережі, машинне навчання, поведінкова економіка, моделі прогнозування.*

Рис.: *6.* ***Бібл.:*** *15.*

Гур'янова Лідія Семенівна *– доктор економічних наук, професор, професор кафедри економічної кібернетики та прикладної економіки, Харківський національний університет імені В. Н. Каразіна (майдан Свободи, 4, Харків, 61022, Україна)*

E-mail: *guryanovalidiya@gmail.com*

ORCID: *https://orcid.org/0000-0002-2009-1451*

Researcher ID: *https://www.webofscience.com/wos/author/record/L-3402-2017*

Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=36068855600*

Луценко Ростислав Русланович *– аспірант кафедри економічної кібернетики та прикладної економіки, Харківський національний університет імені В. Н. Каразіна (майдан Свободи, 4, Харків, 61022, Україна)*

E-mail: *roxanisen@gmail.com*

ORCID: *https://orcid.org/0000-0003-0737-3902*

Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57238374000*