https://doi.org/10.31891/2307-5740-2025-338-79
УДК 336.71:336.76

БЛИЗНЮК Тетяна
Харківський національний економічний університет імені Семена Кузнеця
https://orcid.org/0000-0002-8291-4150
КИРІЙ Валентина
Харківський національний університет радіоелектроніки
https://orcid.org/0000-0002-2537-264X
ГОЛУБКІН Сергій
Державний біотехнологічний університет
https://orcid.org/0009-0002-7673-4943

ФІНАНСОВЕ ШАХРАЙСТВО ЯК ЗАГРОЗА ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: СУЧАСНІ ВИКЛИКИ ТА МЕТОДИ ПРОТИДІЇ

Фінансове шахрайство є однією з найбільших загроз для сучасного бізнес-середовища, зокрема в умовах швидкої цифровізації та глобалізації. Це явище не тільки викликає прямі фінансові втрати, але й створює серйозні репутаційні ризики для підприємств, що негативно позначається на їхній конкурентоспроможності та економічній стабільності. Метою цього дослідження є огляд методів моніторингу фінансових транзакцій та підходів до захисту електронних платежів, а також окреслення рекомендацій для удосконалення цих процесів. Актуальність теми підкріплюється потребою розробки новітніх інструментів контролю, здатних виявляти аномальні транзакції в реальному часі, що стає можливим завдяки застосуванню технологій штучного інтелекту та машинного навчання. Важливим напрямком є інтеграція таких систем у загальну систему фінансової безпеки підприємств. У роботі також розглядаються основні види фінансового шахрайства, включаючи шахрайства з кредитними картками, фінансовою звітністю та страхуванням, а також кіберзлочинність. З огляду на це, для забезпечення належного рівня захисту необхідно поєднувати традиційні методи моніторингу з інноваційними підходами до аналізу даних. Запропоновані підходи можуть значно підвищити захищеність фінансових операцій та знизити ризики шахрайських дій. Окрім того, наукові дослідження повинні сприяти вдосконаленню інтеграції нормативно-правової бази для більш ефективної боротьби з шахрайством на міжнародному рівні.

Ключові слова: фінансове шахрайство; моніторинг транзакцій; штучний інтелект; машинне навчання; фінансова безпека; кіберзлочинність.

BLYZNYUK Tetyana
Simon Kuznets Kharkiv National University of Economics
KYRII Valentyna
Kharkiv National University of Radio Electronics
HOLUBKIN Serhii
State Biotechnological University

FINANCIAL FRAUD AS A THREAT TO THE FINANCIAL SECURITY OF AN ENTERPRISE: MODERN CHALLENGES AND METHODS OF COUNTERACTION

This article is devoted to an in-depth analysis of financial fraud, which poses a significant threat to the modern business environment. The rapid expansion of digital technologies and the globalization of the economy create new opportunities for attackers, which requires constant improvement of methods for monitoring and protecting financial transactions. The study aims to review modern monitoring methods and approaches to protecting electronic payments and develop practical recommendations for their improvement.

The article analyzes in detail the latest research and publications related to the detection of financial anomalies, the application of machine learning algorithms, big data analysis, and other technological solutions. Various types of financial fraud are considered, including fraud with credit cards, financial statements, insurance, cryptocurrencies, and other digital assets. Special attention is paid to analyzing methods for managing the risks of financial transactions, including traditional and modern approaches, such as machine learning and artificial intelligence methods.

The issues of real-time transaction monitoring and post-facto analysis are considered, as well as the importance of forming an explicit data structure and high-quality information collection to detect fraudulent schemes effectively. The conclusions emphasize the need for a multi-level transaction control system that combines preventive measures and in-depth data analysis. Integrating legislation and cooperation between financial institutions for effective counteraction to fraud is also emphasized.

The article offers practical recommendations for improving financial security systems, focusing on adapting to rapidly changing technological and economic conditions. Prospects for further research in this area are considered, including integrating blockchain solutions, quantum cryptography methods, and other innovative technologies to increase the transparency and security of financial transactions.

Keywords: financial fraud, transaction monitoring, electronic payments, machine learning, artificial intelligence, cybersecurity, cryptocurrencies, risk management, financial security, digital technologies.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Фінансове шахрайство перебуває серед найактуальніших загроз для сучасного бізнес-середовища, оскільки швидке розширення цифрових технологій та онлайн-сервісів постійно примножує способи

вчинення злочинних дій. Прямі фінансові втрати, а також репутаційні збитки, спричинені шахрайськими операціями, мають руйнівний вплив на конкурентоспроможність підприємств і стабільність економіки загалом. Глобалізаційні процеси ускладнюють ідентифікацію зловмисників і координацію заходів правового регулювання на міждержавному рівні. У цьому контексті дослідження проблеми фінансового шахрайства та розробка інструментів превентивного контролю, моніторингу та аналітики набувають особливого значення. Застосування методів штучного інтелекту постає критично важливим для виявлення аномальних транзакцій у режимі реального часу, водночас підвищення ефективності інтеграції таких технологій безпосередньо залежить від взаємодії науки, бізнесу та органів державного регулювання.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета - огляд методів моніторингу фінансових транзакцій і підходів до захисту електронних платежів та окреслення практичних рекомендацій щодо їх удосконалення.

Запропоновані підходи можуть бути інтегровані у систему фінансової безпеки підприємств, підвищуючи захищеність електронних операцій та знижуючи рівень можливих ризиків.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Дослідники дедалі більше зосереджуються на питаннях виявлення фінансових аномалій. Значна частина публікацій присвячена застосуванню алгоритмів машинного навчання для ідентифікації нетипових транзакцій і поведінкових патернів, що можуть свідчити про зловживання [1, 2, 5, 6]. Зокрема, у роботах [4, 9, 10] розглядаються різні підходи до класифікації та виявлення аномалій на основі аналізу великих обсягів інформації, а також їх ефективність у контексті швидкої обробки потокових даних. Поряд із цим автори [7, 8, 25] акцентують увагу на проблемі кредитних карток, оскільки висока частота трансакцій і широкий спектр онлайн-сервісів роблять цю сферу особливо вразливою до шахрайських дій. Інший важливий напрям досліджень стосується шахрайства з фінансовою звітністю, страхуванням та операціями у цифровому середовищі (криптовалюти, онлайн-банкінг), де застосування методів глибинного навчання й аналізу графів продемонструвало відчутне зменшення рівня помилкових спрацювань та підвищення ефективності виявлення нетипової активності [15, 16, 20, 21]. Наприклад, у дослідженнях [32, 33, 34, 35] розглядаються підходи до моніторингу руху криптовалют і виявлення підозрілих гаманців, що беруть участь у сумнівних транзакціях. Водночас науковці наголошують на важливості гармонізації нормативно-правової бази та стандартизації процесів обміну інформацією між різними фінансовими установами, оскільки недостатня уніфікація може ускладнювати протидію шахрайству навіть за наявності високотехнологічних рішень [2, 5, 6].

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Фінансове шахрайство - це отримання фінансової вигоди за допомогою незаконних та шахрайських методів [1, 2]. Фінансове шахрайство може здійснюватися в різних сферах, таких як страхування, банківська справа, оподаткування та корпоративний сектор [3]. Останнім часом шахрайство з фінансовими операціями [4], відмивання грошей та інші види фінансового шахрайства [5] стають все більшою проблемою серед компаній та галузей [6]. Незважаючи на численні зусилля, спрямовані на зменшення шахрайської фінансової діяльності, її поширеність негативно впливає на економіку та суспільство, оскільки щодня через шахрайство втрачаються великі суми грошей [6]. Багато років тому було запроваджено кілька підходів до виявлення шахрайства [1]. Більшість традиційних методів є ручними, що є не тільки трудомістким, дорогим і неточним, але й непрактичним [6]. Проводиться все більше досліджень, спрямованих на зменшення втрат від шахрайських дій, але вони не є ефективними [5]. З розвитком підходу штучного інтелекту, машинного навчання та інтелектуального аналізу даних для виявлення шахрайських дій у фінансовому секторі почали використовувати [8, 9].

Шахраї використовують кредитні картки для здійснення незаконних операцій, що призводить до величезних збитків для банків і власників карток [13]. Більше того, винайдення підроблених карток допомогло шахраям здійснювати незаконні операції більш ефективно. Загалом, використання картки без належного дозволу власника вважається незаконним. Отримання доступу до певного рахунку незаконним шляхом робить будь-яку транзакцію шахрайською [7, 12]. Шахрайські дії з кредитними картками можна розділити на два аспекти, а саме: офлайн та онлайн шахрайство [11]. Офлайн-шахрайство полягає в тому, що шахраї здійснюють незаконні операції з викраденими кредитними картками, наприклад, справжніх власників карток, в той час як онлайн-шахраї здійснюють свою діяльність у сфері онлайн-транзакцій через Інтернет [11, 12].

Шахрайство з фінансовою звітністю передбачає підробку фінансових звітів з метою імітування прибутковості [3], мінімізації податків, отримання банківського кредиту [14]. Це також може включати підробку первинних фінансових документів, що містять інформацію про витрати та доходи [15,16], або внутрішні управлінські документи [17, 18, 19]. Різні фінансові документи відображають фінансовий стан підприємства, вказують на те, наскільки воно успішне і допомагає оцінити його кредитоспроможність [15, 16]. Основною метою шахрайства з фінансовою звітністю є підвищення цін на акції, мінімізація податкових

зобов'язань, залучення якомога більшої кількості інвесторів та отримання доступу до банківських кредитів [8].

Страхове шахрайство можна визначити як зловживання страховим полісом для отримання незаконної вигоди від страхового бізнесу [20]. Зазвичай, страхування здійснюється для захисту операцій організації або фізичної особи від будь-яких фінансових ризиків [15, 16]. Основними секторами, на які спрямовані шахрайські страхові вимоги, є охорона здоров'я [5, 21, 22] та автомобільні страхові компанії [23, 24]. Хоча шахрайство у страхуванні житла та врожаю також трапляється [1]. Шахраї-одинаки здатні вчиняти шахрайські дії, і одним із методів вчинення шахрайства є обман під час процесу відшкодування збитків [26]. Іноді організовані групи працюють разом для здійснення страхового шахрайства [10]. Як правило, ці групи інсценують страхові випадки. Тим не менше, більшість випадків шахрайства - випадкові шахрайства, які не плануються; натомість особа користується можливістю, яку надає така аварія, перебільшуючи заявлені суми відшкодування або збитків.

Фінансове кібершахрайство охоплює низку злочинів, які вчиняються в кіберпросторі з метою отримання незаконної економічної вигоди [27, 28]. Злочинців, які вчиняють фінансові кіберзлочини, важко ідентифікувати [29, 30]. Вони навмисно маскують свою діяльність, щоб змішати свої дії з очікуваною поведінкою клієнта або користувача веб-сайту чи фінансової послуги. Оскільки просунуті технології стають доступними для злочинців, тактика вчинення кримінальних правопорушень ускладнюється. Цей симбіоз фінансових шахрайств та кібербезпеки призводить до того, що фінансові установи використовують власні методи захисту [31]. Однак, оскільки підходи до здійснення шахрайств постійно еволюціонують [32], необхідно розробляти та впроваджувати нові методи, такі як моделі машинного навчання та глибокого навчання [29, 30, 31, 32].

Окрім вищезазначених видів шахрайських дій, трапляються й інші шахрайства, до яких належать шахрайство з цінними паперами [14], іпотечне шахрайство [5], корпоративне шахрайство та відмивання грошей [5]. Шахрайство з цінними паперами - це схиляння особи до інвестування в компанію на основі наданої фальшивої інформації [5]. Іпотечне шахрайство - це суттєва неправдива інформація, надана боржником на будь-якому етапі процедури подання заявки для отримання позики або кредиту [5]. Воно навмисно націлене на документи, пов'язані з іпотекою, шляхом зміни інформації під час процесу подання заявки на іпотечний кредит [6]. Іншим поширеним видом шахрайства є корпоративне шахрайство, коли інсайдери фальсифікують фінансові документи для приховування шахрайства або злочинної діяльності [14]. Відмивання грошей - це ще один вид фінансового шахрайства, в якому намагаються підмінити джерело походження коштів [1, 5]. Відмивання грошей суттєво впливає на суспільство, оскільки є основним методом, за допомогою якого здійснюються інші злочини, такі як фінансування тероризму та торгівля зброєю [4, 5]. Іншим поширеним фінансовим злочином є шахрайство з криптовалютою [17, 33, 34]. Основна ідея полягає в тому, щоб заманити невинних людей обіцянкою значних прибутків від їхніх інвестицій [16, 35]. У таблиці 5 наведено різні види фінансового шахрайства.

Зростання ризиків шахрайських операцій у фінансовій сфері зумовлене впливом кількох взаємопов’язаних чинників, серед яких особливе значення має цифровізація. Запровадження електронних платіжних систем, розвиток віртуальних платформ та перехід на онлайн-сервіси прискорюють обіг коштів, проте водночас відкривають нові можливості для зловмисників. Важливу роль відіграють дистанційні канали обслуговування клієнтів, що дають змогу проводити фінансові операції через мобільні додатки, веб-сайти та кол-центри, але підвищують імовірність витоку конфіденційних даних, оскільки користувачі та співробітники не завжди дотримуються належних заходів безпеки. Додатковим чинником виступає глобалізація [17], яка розширює географічні кордони транзакцій та ускладнює контроль за фінансовими потоками. Унаслідок цього міжнародне право та регуляторні органи не встигають ефективно координувати зусилля щодо попередження і виявлення шахрайських схем, що створює сприятливі умови для транснаціональних злочинних угруповань.

У сфері управління ризиками фінансових операцій застосовуються різноманітні підходи, що охоплюють як превентивні [22], так і реактивні [6] заходи. Традиційні методи ризик-менеджменту ґрунтуються на встановленні фіксованих правил і параметрів [20], згідно з якими оцінюється безпечність транзакцій. Такий підхід спирається на заздалегідь визначені шаблони поведінки й може бути ефективним у ситуаціях з відносно стабільним середовищем. Однак у динамічних умовах сучасного ринку він часто не дозволяє оперативно реагувати на появу нових типів шахрайства, оскільки потребує постійного коригування алгоритмів. Своєю чергою, удосконалені системи контролю й аналітики дедалі частіше базуються на методах машинного навчання [26], що дають змогу ідентифікувати аномалії в режимі реального часу та адаптуватися до мінливих схем зловмисників.

Вибір конкретного інструменту моніторингу залежить від масштабу діяльності фінансової установи, рівня захищеності IT-інфраструктури й готовності інвестувати в технології. До базових методів належить комплексний аудит транзакцій з одночасним використанням декількох джерел даних [30], що дає змогу порівнювати параметри операцій із внутрішніми й зовнішніми базами, а також оновлюваними профілями клієнтів. Застосування систем штучного інтелекту підвищує точність виявлення підозрілих операцій за рахунок аналізу неочевидних зв’язків і розширення можливостей обробки великих обсягів інформації. У

підсумку, поєднання традиційних правил і сучасних алгоритмів сприяє формуванню багаторівневої системи безпеки [14], що дає змогу ефективніше контролювати ризики та швидко реагувати на нові загрози у платіжному середовищі.

У процесі аналізу й запобігання порушенням широко застосовуються два ключових підходи. Перший полягає в організації моніторингу транзакцій у режимі реального часу [31], завдяки чому потенційні загрози можна виявляти й блокувати безпосередньо під час обробки платежу. Такий механізм вимагає [35] високої продуктивності системи й здатності обробляти значні обсяги даних миттєво. Другий підхід передбачає здійснення перевірок після завершення фінансової операції [9], що дає змогу зосередитися на детальному аналізі даних у поєднанні з історичною інформацією про клієнтів і попередні операції. Цей підхід дозволяє виявляти складні або приховані схеми шахрайства, які не завжди можна зафіксувати під час виконання транзакції в реальному часі. Оптимальна модель контролю часто [5] включає одночасне використання обох підходів, що дає змогу поєднати оперативне реагування й глибину аналітики.

Для підвищення результативності аналітики вкрай важливим є формування чіткої структури даних і якісне збирання інформації. Ретельне логування всіх етапів обробки транзакцій, зокрема запис подій у журналах і створення аудиторських трас, поліпшує [2] умови для глибинного аналізу у випадку підозри на фальсифікацію. Розподіл даних за попередньо визначеними категоріями та використання уніфікованих форматів спрощують процеси порівняння і дозволяють зосередитися на пошуку відхилень від нормальної поведінки. У підсумку це сприяє побудові більш цілісної системи моніторингу, яка уможливлює своєчасне виявлення навіть складних шахрайських схем.

Швидке поширення нових технологій шахрайства створює умови, за яких традиційні методи захисту не завжди здатні забезпечити належний рівень безпеки [3]. У такій ситуації виникає потреба в оперативній адаптації програмних рішень і оновленні алгоритмів моніторингу. Водночас складність інтеграції різнорідних даних, що надходять із різних платформ та каналів взаємодії, вимагає ретельно розроблених стратегій збору та уніфікації інформації. Без ефективного вирішення цих питань повноцінний аналіз і своєчасне виявлення аномалій стають проблематичними, особливо з огляду на зростання обсягів транзакційного трафіку та появу інноваційних схем зловмисників.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Узагальнюючи результати проведеного дослідження, можна дійти висновку, що фінансове шахрайство залишається одним із найсуттєвіших викликів для сучасних підприємств. Його поширеність зумовлена різноманітністю злочинних схем, які охоплюють як традиційні форми підробки платіжних документів чи звітності, так і кіберзагрози, що стрімко еволюціонують. Активна цифровізація, глобалізація та використання дистанційних каналів обслуговування клієнтів посилюють потребу в багаторівневій системі контролю транзакцій, яка передбачає одночасне застосування превентивних заходів і глибинного аналізу даних у постфактум-режимі. Значну роль у цьому процесі відіграють методи машинного навчання та штучного інтелекту, що дають змогу оперативно виявляти аномальну поведінку й адаптуватися до нових схем зловмисників. Водночас недостатня інтегрованість законодавства у світовому масштабі ускладнює обмін даними та гальмує ефективну протидію шахрайству, особливо за умови транснаціональної діяльності злочинних угруповань.

Подальші напрямки досліджень можуть полягати у вдосконаленні технологій аналізу великих даних, інтеграції блокчейн-рішень та квантових методів криптографії, що здатні підвищити рівень прозорості та безпеки фінансових операцій. Комплексне поєднання правового регулювання, технічних інновацій і процедур внутрішнього контролю має стати основою для формування більш надійної системи захисту від фінансового шахрайства.

Література

1. Hilal W., Gadsden S. A., Yawney J. Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. Expert Syst. Appl. 2021, 193, 116429. DOI: https://doi.org/10.1016/j.eswa.2021.116429

2. Ashtiani M. N., Raahemi B. Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review. IEEE Access 2021, 10, 72504–72525. DOI: http://doi.org/10.1109/ACCESS.2021.3096799

3. Albashrawi M. Detecting Financial Fraud Using Data Mining Techniques: A Decade Review from 2004 to 2015. J. Data Sci. 2016, 14, 553–570. DOI: https://doi.org/10.6339/JDS.201607_14(3).0010

4. Choi D., Lee K. An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation. Secur. Commun. Netw. 2018, 2018, 1–15. DOI: https://doi.org/10.1155/2018/5483472

5. Ngai E.W., Hu Y., Wong Y. H., Chen Y., Sun X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decis. Support Syst. 2011, 50, 559–569. DOI: http://dx.doi.org/10.1016/j.dss.2010.08.006

6. Al-Hashedi K. G., Magalingam P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Comput. Sci. Rev. 2021, 40, 100402. DOI: https://doi.org/10.1016/j.cosrev.2021.100402
7. Delamaire L., Hussein A., John P. Credit card fraud and detection techniques: A review. Banks Bank Syst. 2009, 4, 57–68. URL: https://salford-repository.worktribe.com/output/1465545
8. West J., Bhattacharya M. Intelligent financial fraud detection: A comprehensive review. Comput. Secur. 2016, 57, 47–66. DOI: https://doi.org/10.1016/j.cose.2015.09.005
9. Abdallah A., Maarof M. A., Zainal A. Fraud detection system: A survey. J. Netw. Comput. Appl. 2016, 68, 90–113. DOI: https://doi.org/10.1016/j.jnca.2016.04.007
10. Pourhabibi T., Ong K. L., Kam B. H., Boo Y. L. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decis. Support Syst. 2020, 133, 113303. DOI: https://doi.org/10.1016/j.dss.2020.113303
11. Bhattacharyya S., Jha S., Tharakunnel K., Westland J. C. Data mining for credit card fraud: A comparative study. Decis. Support Syst. 2011, 50, 602–613. DOI: https://doi.org/10.1016/j.dss.2010.08.008
12. Srivastava A., Yadav M., Basu S., Salunkhe S., Shabad M. Credit card fraud detection at merchant side using neural networks. In Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016; pp. 667–670. URL: https://ieeexplore.ieee.org/abstract/document/7724348
13. Sá A. G., Pereira A. C., Pappa G. L. A customized classification algorithm for credit card fraud detection. Eng. Appl. Artif. Intell. 2018, 72, 21–29. DOI: https://doi.org/10.1016/j.engappai.2018.03.011
14. Robinson W. N., Aria A. Sequential fraud detection for prepaid cards using hidden Markov model divergence. Expert Syst. Appl. 2018, 91, 235–251. DOI: https://doi.org/10.1016/j.eswa.2017.08.043
15. Hajek P., Henriques R. Mining corporate annual reports for intelligent detection of financial statement fraud — A comparative study of machine learning methods. Knowl.-Based Syst. 2017, 128, 139–152. DOI: https://doi.org/10.1016/j.knosys.2017.05.001
16. Craja P., Kim, A., Lessmann S. Deep learning for detecting financial statement fraud. Decis. Support Syst. 2020, 139, 113421. DOI: https://doi.org/10.1016/j.dss.2020.113421
17. Ravisankar P., Ravi V., Rao G. R., Bose I. Detection of fi nancial statement fraud and feature selection using data mining techniques. Decis. Support Syst. 2011, 50, 491–500. DOI: https://www.sciencedirect.com/science/article/pii/S0167923610001879
18. Gao Y., Sun C., Li R., Li Q., Cui L., Gong B. An Efficient Fraud Identification Method Combining Manifold Learning and Outliers Detection in Mobile Healthcare Services. IEEE Access 2018, 6, 60059–60068. URL: https://ieeexplore.ieee.org/abstract/document/8489846
19. Huang S. Y., Tsaih R. H., Yu F. Topological pattern discovery and feature extraction for fraudulent financial reporting. Expert Syst. Appl. 2014, 41, 4360–4372. DOI: https://doi.org/10.1016/j.eswa.2014.01.012
20. Peng J., Li Q., Li H., Liu L., Yan Z., Zhang S. Fraud Detection of Medical Insurance Employing Outlier Analysis. In Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanjing, China, 9–11 May 2018; pp. 341–346. URL: https://ieeexplore.ieee.org/abstract/document/8465273
21. Van Capelleveen G., Poel M., Mueller R. M., Thornton D., van Hillegersberg J. Outlier detection in healthcare fraud: A case study in the Medicaid dental domain. Int. J. Account. Inf. Syst. 2016, 21, 18–31. DOI: https://doi.org/10.1016/j.accinf.2016.04.001
22. Anbarasi M. S., Dhivya S. Fraud detection using outlier predictor in health insurance data. In Proceedings of the 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 23–24 February 2017; pp. 1–6. URL: https://ieeexplore.ieee.org/abstract/document/8070750
23. Sundarkumar G. G., Ravi V., Siddeshwar V. One-class support vector machine based undersampling: Application to churn prediction and insurance fraud detection. In Proceedings of the 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 10–12 December 2015; pp. 1–7. URL: https://ieeexplore.ieee.org/abstract/document/7435726
24. Subudhi S., Panigrahi S. Effect of Class Imbalanceness in Detecting Automobile Insurance Fraud. In Proceedings of the 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA), ChangSha, China, 21–23 September 2018; pp. 528–531. URL: https://ieeexplore.ieee.org/abstract/document/8588973
25. Fayyomi M., Eleyan D., Eleyan A. A Survey Paper On Credit Card Fraud Detection Techniques. Int. J. Adv. Res. Comput. Eng. Technol. 2021, 3, 827–832. URL: https://www.academia.edu/download/92975520/A-Survey-Paper-On-Credit-Card-Fraud-Detection-Techniques.pdf
26. Wang Y., Xu W. Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. Decis. Support Syst. 2018, 105, 87–95. DOI: https://doi.org/10.1016/j.dss.2017.11.001

27. Gepp A., Kumar K., Bhattacharya S. Lifting the numbers game: Identifying key input variables and a best-performing model to detect financial statement fraud. Account. Financ. 2021, 61, 4601–4638. DOI: https://doi.org/10.1111/acfi.12742

28. Perols L., Lougee B. A. The relation between earnings management and financial statement fraud. Adv. Account. 2011, 27, 39–53. DOI: https://doi.org/10.1016/j.adiac.2010.10.004

29. Wang Q., Xu W., Huang X., Yang K. Enhancing intraday stock price manipulation detection by leveraging recurrent neural networks with ensemble learning. Neurocomputing 2019, 347, 46–58. DOI: https://doi.org/10.1016/j.neucom.2019.03.006

30. Islam S. R., Ghafoor S. K., Eberle W. Mining Illegal Insider Trading of Stocks: A Proactive Approach. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 1397–1406. URL: https://ieeexplore.ieee.org/abstract/document/8622303

31. Kulkarni P. M., Domeniconi C. Network-based anomaly detection for insider trading. arXiv. 2017. DOI: https://doi.org/10.48550/arXiv.1702.05809

32. Mirtaheri M., Abu-El-Haija S., Morstatter F., Steeg G. V., Galstyan, A. Identifying and Analyzing Cryptocurrency Manipulations in Social Media. IEEE Trans. Comput. Soc. Syst. 2021, 8, 607–617. URL: https://ieeexplore.ieee.org/abstract/document/9371307

33. Monamo P. M., Marivate V., Twala B. A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers. In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 188–194. URL: https://ieeexplore.ieee.org/abstract/document/7838143

34. Vasek M., Moore T. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams BT–Financial Cryptography and Data Security. In Proceedings of the International Conference on Financial Cryptography and Data Security, Kota Kinabalu, Malaysia, 1–5 March 2015; pp. 44–61. URL: https://tylermoore.utulsa.edu/fc15.pdf

35. Monamo P., Marivate V., Twala B. Unsupervised learning for robust Bitcoin fraud detection. In Proceedings of the 2016 Information Security for South Africa (ISSA), Johannesburg, South Africa, 17–18 August 2016; pp. 129–134. URL: https://ieeexplore.ieee.org/abstract/document/7802939

Refereces

1. Hilal, W., Gadsden, S. A., & Yawney, J. (2021). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications, 193*, 116429. https://doi.org/10.1016/j.eswa.2021.116429

2. Ashtiani, M. N., & Raahemi, B. (2021). Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review. *IEEE Access, 10*, 72504–72525. http://doi.org/10.1109/ACCESS.2021.3096799

3. Albashrawi, M. (2016). Detecting financial fraud using data mining techniques: A decade review from 2004 to 2015. *Journal of Data Science, 14*, 553–570. https://doi.org/10.6339/JDS.201607_14(3).0010

4. Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. *Security and Communication Networks, 2018*, 1–15. https://doi.org/10.1155/2018/5483472

5. Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*, 559–569. http://dx.doi.org/10.1016/j.dss.2010.08.006

6. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review, 40*, 100402. https://doi.org/10.1016/j.cosrev.2021.100402

7. Delamaire, L., Hussein, A., & John, P. (2009). Credit card fraud and detection techniques: A review. *Banks and Bank Systems, 4*, 57–68. https://salford-repository.worktribe.com/output/1465545

8. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security, 57*, 47–66. https://doi.org/10.1016/j.cose.2015.09.005

9. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications, 68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

10. Pourhabibi, T., Ong, K. L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems, 133*, 113303. https://doi.org/10.1016/j.dss.2020.113303

11. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*, 602–613. https://doi.org/10.1016/j.dss.2010.08.008

12. Srivastava, A., Yadav, M., Basu, S., Salunkhe, S., & Shabad, M. (2016). Credit card fraud detection at merchant side using neural networks. In *Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 667–670). https://ieeexplore.ieee.org/abstract/document/7724348

13. Sá, A. G., Pereira, A. C., & Pappa, G. L. (2018). A customized classification algorithm for credit card fraud detection. *Engineering Applications of Artificial Intelligence, 72*, 21–29. https://doi.org/10.1016/j.engappai.2018.03.011

14. Robinson, W. N., & Aria, A. (2018). Sequential fraud detection for prepaid cards using hidden Markov model divergence. *Expert Systems with Applications, 91*, 235–251. https://doi.org/10.1016/j.eswa.2017.08.043

15. Hajek, P., & Henriques, R. (2017). Mining corporate annual reports for intelligent detection of financial statement fraud — A comparative study of machine learning methods. *Knowledge-Based Systems, 128*, 139–152. https://doi.org/10.1016/j.knosys.2017.05.001

16. Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud. *Decision Support Systems, 139*, 113421. https://doi.org/10.1016/j.dss.2020.113421

17. Ravisankar, P., Ravi, V., Rao, G. R., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision Support Systems, 50*, 491–500. https://www.sciencedirect.com/science/article/pii/S0167923610001879

18. Gao, Y., Sun, C., Li, R., Li, Q., Cui, L., & Gong, B. (2018). An efficient fraud identification method combining manifold learning and outliers detection in mobile healthcare services. *IEEE Access, 6*, 60059–60068. https://ieeexplore.ieee.org/abstract/document/8489846

19. Huang, S. Y., Tsaih, R. H., & Yu, F. (2014). Topological pattern discovery and feature extraction for fraudulent financial reporting. *Expert Systems with Applications, 41*, 4360–4372. https://doi.org/10.1016/j.eswa.2014.01.012
20. Peng, J., Li, Q., Li, H., Liu, L., Yan, Z., & Zhang, S. (2018). Fraud detection of medical insurance employing outlier analysis. In *Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD)* (pp. 341–346). https://ieeexplore.ieee.org/abstract/document/8465273
21. Van Capelleveen, G., Poel, M., Mueller, R. M., Thornton, D., & van Hillegersberg, J. (2016). Outlier detection in healthcare fraud: A case study in the Medicaid dental domain. *International Journal of Accounting Information Systems, 21*, 18–31. https://doi.org/10.1016/j.accinf.2016.04.001
22. Anbarasi, M. S., & Dhivya, S. (2017). Fraud detection using outlier predictor in health insurance data. In *Proceedings of the 2017 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 1–6). https://ieeexplore.ieee.org/abstract/document/8070750
23. Sundarkumar, G. G., Ravi, V., & Siddeshwar, V. (2015). One-class support vector machine based undersampling: Application to churn prediction and insurance fraud detection. In *Proceedings of the 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1–7). https://ieeexplore.ieee.org/abstract/document/7435726
24. Subudhi, S., & Panigrahi, S. (2018). Effect of class imbalance in detecting automobile insurance fraud. In *Proceedings of the 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA)* (pp. 528–531). https://ieeexplore.ieee.org/abstract/document/8588973
25. Fayyomi, M., Eleyan, D., & Eleyan, A. (2021). A survey paper on credit card fraud detection techniques. *International Journal of Advanced Research in Computer Engineering & Technology, 3*, 827–832. https://www.academia.edu/download/92975520/A-Survey-Paper-On-Credit-Card-Fraud-Detection-Techniques.pdf
26. Wang, Y., & Xu, W. (2018). Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. *Decision Support Systems, 105*, 87–95. https://doi.org/10.1016/j.dss.2017.11.001
27. Gepp, A., Kumar, K., & Bhattacharya, S. (2021). Lifting the numbers game: Identifying key input variables and a best-performing model to detect financial statement fraud. *Accounting and Finance, 61*, 4601–4638. https://doi.org/10.1111/acfi.12742
28. Perols, L., & Lougee, B. A. (2011). The relation between earnings management and financial statement fraud. *Advances in Accounting, 27*, 39–53. https://doi.org/10.1016/j.adiac.2010.10.004
29. Wang, Q., Xu, W., Huang, X., & Yang, K. (2019). Enhancing intraday stock price manipulation detection by leveraging recurrent neural networks with ensemble learning. *Neurocomputing, 347*, 46–58. https://doi.org/10.1016/j.neucom.2019.03.006
30. Islam, S. R., Ghafoor, S. K., & Eberle, W. (2018). Mining illegal insider trading of stocks: A proactive approach. In *Proceedings of the 2018 IEEE International Conference on Big Data (Big Data)* (pp. 1397–1406). https://ieeexplore.ieee.org/abstract/document/8622303
31. Kulkarni, P. M., & Domeniconi, C. (2017). Network-based anomaly detection for insider trading. *arXiv*. https://doi.org/10.48550/arXiv.1702.05809
32. Mirtaheri, M., Abu-El-Haija, S., Morstatter, F., Steeg, G. V., & Galstyan, A. (2021). Identifying and analyzing cryptocurrency manipulations in social media. *IEEE Transactions on Computational Social Systems, 8*, 607–617. https://ieeexplore.ieee.org/abstract/document/9371307
33. Monamo, P. M., Marivate, V., & Twala, B. (2016). A multifaceted approach to Bitcoin fraud detection: Global and local outliers. In *Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 188–194). https://ieeexplore.ieee.org/abstract/document/7838143
34. Vasek, M., & Moore, T. (2015). There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In *Proceedings of the International Conference on Financial Cryptography and Data Security* (pp. 44–61). https://tylermoore.utulsa.edu/fc15.pdf
35. Monamo, P., Marivate, V., & Twala, B. (2016). Unsupervised learning for robust Bitcoin fraud detection. In *Proceedings of the 2016 Information Security for South Africa (ISSA)* (pp. 129–134). https://ieeexplore.ieee.org/abstract/document/7802939