УДК 330.65
DOI: https://doi.org/10.32782/1814-1161/2025-4-20

Шуляр Р.В.
доктор економічних наук, професор,
професор кафедри менеджменту і міжнародного підприємництва
Національного університету «Львівська політехніка»
ORCID: https://orcid.org/0000-0001-8065-7579

Харчук В.Ю.
аспірант
Національного університету «Львівська політехніка»
ORCID: https://orcid.org/0009-0005-5515-5135

Гайдук Б.В.
аспірант
Національного університету «Львівська політехніка»
ORCID: https://orcid.org/0009-0007-5774-6574

Shuliar Roman
Doctor of Economics, Professor,
Professor of the Management and International Business Department
Lviv Polytechnic National University

Kharchuk Vitalii
Postgraduate Student
Lviv Polytechnic National University

Haiduk Bohdan
Postgraduate Student
Lviv Polytechnic National University

АНАЛІЗУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ З УПРАВЛІННЯ КОМПЛАЄНС-РИЗИКАМИ ОРГАНІЗАЦІЇ

ANALYSIS OF INFORMATION SYSTEMS FOR COMPLIANCE RISK MANAGEMENT OF THE ORGANIZATION

Управління комплаєнс-ризиками є одним із найбільш гострих завдань в організації, що зумовлено як мінливістю та багатоаспектністю національної та міжнародної нормативно-правової бази, так і зміною парадигми використання інформаційних систем в ризик-менеджменті. Власне вирішенню окресленої проблематики і присвячені дані наукові розвідки. Стаття досліджує існуючі інформаційні системи, придатні для підтримки та оптимізації процедур управління комплаєнс-ризиками в організації. Зокрема проаналізовано інформаційні системи Управління, Ризик та Комплаєнс (GRC), Системи з Комплаєнс Менеджменту (CMS), Системи безперервного Моніторингу Контролю (CCM) та Безперервного Аудиту (CA), Системи та рішення RegTech з позиції окреслення сильних та слабких сторін означених систем в процесі застосування в організаціях. На основі отриманих результатів розвинуто рекомендації українським організаціям, з приводу використання інформаційних систем у своїй діяльності для удосконалення управління комплаєнс-ризиками.

Ключові слова: *комплаєнс, комплаєнс-ризик, ризик-менеджмент, інформаційні системи, цифрові рішення.*

Compliance risk management is one of the most pressing tasks in an organisation, due to both the variability and multifaceted nature of the national and international regulatory framework, as well as the shift in the paradigm of using information systems in risk management. The article examines existing information systems suitable for supporting and optimising compliance risk management procedures in an organisation. In particular, the information systems Governance, Risk and Compliance (GRC), Compliance Management Systems (CMS), Continuous Control Monitoring (CCM) and Continuous Audit (CA) Systems, RegTech Systems and Solutions are analysed from the standpoint of outlining the strengths and weaknesses of the aforementioned systems in the process of application in organisations. Analysis of information systems suitable for compliance risk management reveals that, today, an organisation has a wide range of options. At the same time, they differ in terms of business process coverage, implementation and configuration flexibility, functionality, cost, and level of employee involvement. Typical weaknesses

of information systems today include the integration of all necessary data for analysis in a single repository, the cleaning and protection of such data, the potential for algorithmic bias, and the involvement of employees in the validation of the results obtained. Based on the given results, the authors developed recommendations aimed at improving the use of information systems by Ukrainian organisations to enhance compliance risk management. First and foremost, it is recommended to identify the goal, objectives and business processes and align compliance, risk management, internal audit, legal support, and operational activities with the goals of company management. Secondly, to develop an organisation's data warehouse that will be updated on an ongoing basis and will combine both the organisation's internal data (data on transactions, customers, partners, suppliers, etc.) and external data (the regulatory and legal framework that regulates the organisation's activities and its interaction with stakeholders, reporting, communication, data storage and use, etc.). Last but not least, to develop a data management policy that will contain information on the procedure for storing, using, and cleaning data and assess the cost and effectiveness of existing compliance risk management information systems and track the potential impact of such systems on the key performance indicators of the organisation as a whole.

Keywords: *compliance, compliance risk, risk management, information systems, digital solutions.*

Постановка проблеми. Дослідження питань використання інформаційних систем для підтримання та забезпечення надійного підґрунтя управління комплаєнс-ризиками, на сьогодні, є надзвичайно актуальним. Першочергово, це зумовлено, власне, самою природою комплаєнс-ризиків, які виникають у випадку недотримання організацією нормативно-правових актів, загальновизнаних стандартів, правил й процедур. Як наслідок, останнє потребує прискіпливого відслідковування усіх змін в нормативних документах, аналізування впливу цих змін на діяльність організації, опрацювання великого масиву даних та, за необхідності, застосування превентивних заходів. По друге, сучасні умови ведення бізнесу та динамічний розвиток цифрових інструментів зумовлюють необхідність використання та системного оновлення IT систем як для управління організацією в цілому, так і управління ризиками зокрема. По третє, на сьогодні актуалізується питання забезпечення прозорості та узгодження процедур ризик-менеджменту із внутрішнім аудитом, юридичним супроводом та операційною діяльністю.

Аналіз останніх досліджень і публікацій. Проблематика використання інформаційних систем та технологій для забезпечення процедур управління комплаєнс-ризиками досліджувалась у працях українських науковців. Зокрема, дослідник Осаволюк О. [1] приділив увагу вивченню особливостей застосування IT-систем в процесі управління податкових комплаєнс-ризиків. Так автор звертає увагу на доцільність використання таких систем як: аналізу великих даних; автоматизації податкового аудиту; машинного навчання й штучного інтелекту; хмарні обчислювальні платформи; інтегровані блок-чейн технології; електронного обліку та звітності [1]. У науковій праці [2] акцент робиться на необхідності створення в організації комплаєнс-служби, яка б оперувала чотирьома основними стратегіями захисту бізнес-процесів від комплаєнс-ризиків. Цікаве дослідження провели Papazafeiropoulou A. та Spanaki K. [3], які звертають увагу на інтегровані системи управління, ризиків та комплаєнсу (Governance, Risk and Compliance Information Systems (GRC IS), їхні характеристики та особливості імплементації в діяльності суб'єктів господарювання. Заслуговують уваги результати досліджень Viracacha Pena та Jeimmy Lorena [4], де автори піднімають проблематику використання RegTech для забезпечення процедур управління комплаєн-ризиками [4]. Автори вказують, що під RegTech зазвичай розуміють використання технологій з метою підвищення ефективності та результативності процесів забезпечення комрлаєнсу [4].

В цілому слід зазначити, що у закордонній науковій літературі протягом останнього часу приділено чимало уваги використанню різноманітних IT систем, націлених на забезпечення процесів дотримання нормативних вимог. В той час як в українській науковій царині дана проблематика є менш висвітленою та потребує детального вивчення не лише з точки зору розуміння сучасних інформаційних систем, придатних для підтримання комплаєнс ризик-менеджменту, а й вироблення рекомендацій для вітчизняних організацій з практичної інтеграції таких систем.

Метою статті є дослідження інформаційних систем, націлених на підтримку управління комплаєнс-ризиками організації та здійснення, на цій основі, аналізування існуючих цифрових рішень з точки зору їх сильних сторін та вузьких місць з метою розроблення рекомендацій вітчизняним організаціям у напрямку більш раціонального використання таких систем у своїй діяльності.

Виклад основних результатів дослідження. Загальновідомо, що управління комплаєнс-ризиками передбачає ідентифікування як ризикоутворювальних факторів, так і, власне, самих коплаєнс-ризиків, їхнє оцінювання, моніторинг рівня та динаміки комплаєнс-ризиків з наступною імплементацією відповідних заходів реагування на них [5]. У зв'язку з невпинним зростанням кількості нормативних актів, їхньої мінливості, глобалізаційними процесами у сфері нормативно-правового забезпечення бізнесу, появі нових міжнародних стандартів, з приводу фіксації ризиків, діджиталіязацією бізнес-процесів стає зрозумілим, що традиційні процеси відслідковування дотримання організаціями відповідності є недостатніми та потребують удосконалення [6]. На додачу, за останнє десятиліття комплаєнс перетворився із звиклого контролювання на стратегічну діяльність як у сфері ризик-менеджменту, так і управління організацією в цілому. Таким чином, саме

інформаційні системи (ІС) відіграватимуть ключову роль в автоматизації процесів відслідковування комплаєнс-ризиків організації, моніторингу та інтеграції регуляторної аналітики та здійсненні нагляду в режимі реального часу за усіма бізнес-процесами організації [3, 6].

Варто відмітити, що інформаційні системи, які можуть використовуватись для підтримання управління комплаєнс-ризиками, різнитимуться в залежності від масштабів охоплення бізнес-процесів, інтегрованих спеціалізованих інструментів для моніторингу та оцінювання сфер виникнення таких ризиків, дотримання міжнародних стандартів (наприклад ISO 37301, COSO, GDPR, SOX тощо), підходами до захисту даних та забезпечення цифрової відповідності організації, доступом третіх осіб тощо [3, 6].

На основі аналізування напрацювань вітчизняних та іноземних науковців, міжнародних стандартів, присвячених комплаєнсу, а також практики використання ІТ систем в управлінні комплаєнс-ризиками стає можливим систематизувати інформаційні системи, націлені на управління комплаєнс-ризиками [1–6, 8–12].

1. Системи Управління, Ризик та Комплаєнс (GRC) [3–4] націлені на інтегрування завдань та функцій з управління бізнес-процесами організації, ризик-менеджменту та комплаєнсу. Зокрема, такі системи дозволяють вести централізовані реєстри ризиків та їхнього контролю, автоматизувати процеси із затвердження політик, процедур та звітності про інциденти (в розрізі ризикоутворювальних факторів та ризиків), здійснювати одночасний моніторинг та співставлення дотримання комплаєнсу та ключових індикаторів ризиків (KRI), провадити своєчасне реагування на регуляторні зміни тощо. Серед основних переваг даних систем є інтеграція процедур управління комплаєнс-ризиками із ризик-менеджментом та управлінням організацією в цілому. Як зазначають дослідники [3], серед основних недоліків варто виділити те, що дані системи більшою мірою фокусуються на документації, ніж на ефективності контролю в режимі реального часу. Успіх таких систем також значно визначатиметься від якості та масштабів інтегрованих даних. Серед найбільш популярних систем даного класу можна виділити Optial GRC SmartStart, ServiceNow GRC, RSA Archer, SAP GRC тощо [7].

2. Системи з Комплаєнс Менеджменту (CMS) [8] являють собою інформаційно-технологічні фреймворки, які допомагають здійснювати моніторинг та контроль за дотриманням організацією правових, регуляторних та внутрішніх політик, правил, стандартів тощо. Основним завданням таких систем є зіставлення нормативно-правових документів із внутрішніми політиками/процедурами/стандартами, аналізування можливих відхилень та ідентифікація ризиків, автоматизація повторюваних операцій, документування критичних випадків та, як наслідок, підвищити операційну ефективність організації. Серед слабких місць – фокус лише на комплаєнс ризиках [8]. До систем даного класу належать NAVEX Global, ComplySci, LogicManager, SAI360 [9].

3. Системи безперервного Моніторингу Контролю (CCM) та Безперервного Аудиту (CA) [9–10] здійснюють автоматизацію процесів, пов'язаних із моніторингом фінансових операцій, рівнем та напрямками здійснення витрат, дотриманням нормативно-правових актів та процедурами внутрішнього аудиту. Серед сильних сторін даних систем варто підкреслити здатність виявлення невідповідностей/порушень на ранніх стадіях та усунення рутинних завдань. До слабких сторін даних систем можна віднести потенційно високу вартість обробки значного масиву даних та їхню інтеграцію у бізнес-процеси організації [10]. Серед систем даного класу можна виділити Cyber Sierra, Quod Orbis, Panaseer, SAP Process Control [9–10].

4. Системи та рішення RegTech (регуляторні технології) [4; 11–12] із використанням штучного інтелекту (ШІ) та машинного навчання (МН) забезпечують автоматизацію широкого спектру завдань та процесів, націлених на моніторинг змін в нормативних вимогах, відповідності та моніторингу періодичної фінансової та нефінансової звітності, моніторингу транзакції та їх відповідності загальновизнаним міжнародним стандартам та національному законодавству та виявлення потенційних ризиків та загроз отримання санкцій/штрафів. Разом з тим, опираючись на ШІ та МН організації отримують змогу аналізувати дані з фінансових ринків, платіжних систем, взаємодії з клієнтами та окреслити ключові зобов'язання організації, визначені нормативно-правовими документами з довгостроковим часовим горизонтом [11]. Водночас, останнє може сприяти побудові прогнозних моделей щодо виявлення витоку (потенційного витоку) інсайдерської інформації, існуючих шахрайських схем та інших видів фінансових ризиків [11]. Серед основних переваг таких систем та рішень є проактивний підхід до ідентифікації комплаєнс-ризиків, оптимізація витрат на комплаєнс та використання людських ресурсів, залучених до виконання завдань з управління комплаєнс-ризиками в організації [12]. Серед слабких сторін варто звернути увагу на забезпечення конфіденційності даних, кібербезпеки та можливу алгоритмічну упередженість [12]. Серед найбільш популярних систем даного класу можна виділити Jumio, Onfido, Thomson Reuters, FICO тощо [13].

На основі проведеного аналізування стає можливим окреслення рекомендацій українським організаціям, з приводу використання інформаційних систем у своїй діяльності для удосконалення управління комплаєнс-ризиками:

1. Визначити мету, завдання та бізнес-процеси, які, на думку організації, першочергово потрібно адресувати та удосконалити при допомозі використання сучасних інформаційних систем.

2. Узгодити процедури комплаєнсу, ризик-менеджменту, внутрішнього аудиту, юридичного супроводу, операційної діяльності із цілями управління компанією та окреслити, на цій основі, регуляторні сфери (аспекти в діяльності, які під-

падають під дію аналогічного нормативно-правового забезпечення), які доцільно автоматизувати та здійснювати постійний моніторинг.

3. Розвинути/створити сховище даних організації, яке оновлюватиметься на постійній основі та поєднуватиме як внутрішні дані організації (дані по транзакціях, клієнтах, партнерах, постачальників тощо) та зовнішні дані (нормативно-правова база, яка регламентує діяльність організації та її взаємодію із стейкхолдерами, звітність, комунікацію, зберігання та використання даних тощо).

4. Розвинути/створити політику управління даними, яка міститиме інформацію стосовно порядку зберігання, використання, очищення та недопущення витоку даних та відповідального використання інструментів ШІ, відповідно до загальновизнаних міжнародних стандартів.

5. Здійснити оцінку вартості та ефективності існуючих інформаційних систем з управління комплаєнс-ризиками та простежити потенційних вплив таких систем на ключові показники ефективності організації в цілому.

Висновки. Використання інформаційних систем у підтримці бізнес-процесів організації є об'єктивною вимогою сьогодення. Водночас, коли мова йде про мінливість та різновекторність нормативно-правового забезпечення та множину різноманітних викликів та загроз у сфері комплаєнсу, застосування сучасних інформаційних систем для управління ризиками у даній сфері є вкрай необхідною. Разом з тим, динамічний розвиток цифрових рішень створює не лише додаткові можливості для оптимізації бізнес-процесів та сприяє прийняттю проактивних рішень у сфері управління комплаєнс-ризиками, а може містити як явні, так і приховані загрози для організації. Аналіз інформаційних систем придатних для управління комплаєнс-ризиками свідчить, що, на сьогодні, в організації є широкий вибір опцій, але вони різняться масштабом охоплення бізнес-процесів, гнучкістю впровадження та налаштування в процесі використання, функціоналом, вартістю та рівнем залучення працівників. Спільними слабкими сторонами інформаційних систем, на сьогодні, є інтеграція усіх потрібних даних для аналізування в єдиному сховищі, очищення та захист таких даних, можлива алгоритмічна упередженість та залученість працівників до валідації отриманих результатів. Незважаючи на зазначені аргументи впровадження інформаційних систем для удосконалення управління комплаєнс-ризиками є стратегічною необхідністю та наступні кроки дослідження будуть присвячені даній проблематиці.

Бібліографічний список:

1. Осаволюк О. Застосування іт-систем при управлінні комплаєнс-ризиками. *Молодий вчений.* 2024. № 5 (129). С. 97–101. DOI: https://doi.org/10.32839/2304-5809/2024-5-129-3
2. Кобєлєва Т. О. Стратегії забезпечення комплаєнс-безпеки промислового підприємства. *Economic journal Odessa polytechnic university. Економічний журнал Одеського політехнічного університету.* 2019. № 3 (9). С. 53–61.
3. Papazafeiropoulou A., Spanaki K. Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers.* 2016. № 18. P. 1251–1263. DOI: https://doi.org/10.1007/s10796-015-9572-3
4. Viracacha Pena, Jeimmy Lorena/ Artificial Intelligence in RegTech: Transforming Automated Compliance Audits. SSRN. 2024. URL: https://ssrn.com/abstract=5176055 (дата звернення 25.10.2025).
5. Кузьмін О.Є., Чернобай Л.І., Харчук В.Ю. Економічне оцінювання та планування ризику нововведень на підприємствах машинобудування: монографія. Львів: Видво «РАСТР – 7», 2011. 240 с.
6. Харчук В.Ю. Нормативно-правове підґрунтя врахування комплаєнс-ризику у бізнес-процесах організацій. *Наука і техніка сьогодні*. 2024. № 3 (31). С. 416–426.
7. Top 8 GRC Tools in 2025: A Comprehensive Comparison. URL: https://www.optial.com/resources/top-grc-tools-2025 (дата звернення: 25.10.2025).
8. Malcolm Gammisch, Signe Balina, The Effectiveness of Compliance Management Systems – An Experimental Approach. *Procedia – Social and Behavioral Sciences.* 2014. Volume 156. P. 236–240. DOI: https://doi.org/10.1016/j.sbspro.2014.11.181
9. Ethics And Compliance Software Market Research Report 2033. *Dataintelo*: веб-сайт. URL: https://dataintelo.com/report/ethics-and-compliance-software-market (дата звернення: 25.10.2025).
10. Lombardi D. R., Vasarhelyi M. A.,Begg, I. Continuous Controls Monitoring: A Case Study. *Journal of Emerging Technologies in Accounting*. 2014. № 11 (1). P. 83–98. DOI: https://doi.org/10.2308/jeta-51006
11. Eniola K., Okunola A., Gery, B. AI-driven regulatory technology (RegTech): Streamlining compliance and risk management in the financial sector [Manuscript]. *ResearchGate*. 2025. URL: https://www.researchgate.net/publication/390450097. (дата звернення: 25.10.2025).
12. Chitraju Gopal Varma, Santhosh. The Future of AI-Enabled RegTech in U.S. Financial Markets. [Preprint]. *ResearchGate*. DOI: https://doi.org/10.13140/RG.2.2.30081.77929 (дата звернення: 25.10.2025).
13. What is RegTech and Why It Matters for Financial Services. *Codist*: веб-сайт. URL: https://www.codiste.com/what-is-regtech-guide-compliance-automation (дата звернення: 25.10.2025).

References:

1. Osavolyuk, O. (2024). Zastosuvannia it-system pry upravlinni komplaiens-ryzykamy [Application of it systems in compliance risk management]. *Young Scientist*, no. 5 (129), pp. 97–101. DOI: https://doi.org/10.32839/2304-5809/2024-5-129-3
2. Kobielieva, T. O. (2019). Stratehii zabezpechennia komplaiens-bezpeky promyslovoho pidpryiemstva. [Strategies for ensuring compliance and security of an industrial enterprise] *Economic journal Odessa polytechnic university. Ekonomichnyi zhurnal Odeskoho politekhnichnoho universytetu*, no. 3 (9), pp. 53–61.
3. Papazafeiropoulou, A., Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, no. 18, pp. 1251–1263. DOI: https://doi.org/10.1007/s10796-015-9572-3.
4. Viracacha, Pena, Jeimmy, Lorena (2024). Artificial Intelligence in RegTech: Transforming Automated Compliance. *SSRN.* Available at: https://ssrn.com/abstract=5176055 (accessed October 25 2025).
5. Kuzmin, O.Ie., Chernobai, L.I., Kharchuk, V.Iu. (2011). Ekonomichne otsiniuvannia ta planuvannia ryzyku novovveden na pidpryiemstvakh mashynobuduvannia: monohrafiia [Economic assessment and risk planning of innovations at mechanical engineering enterprises]. Lviv: Vyd-vo "RASTR – 7",. 240 p.

6. Kharchuk, V. Iu. (2024). Normatyvno-pravove pidgruntia vrakhuvannia komplaiens-ryzyku u biznes-protsesakh orhanizatsii [Regulatory and legal basis for taking into account compliance risk in business processes of organizations]. *Nauka i tekhnika sohodni.* no. 3 (31). pp. 416–426.
7. Top 8 GRC Tools in 2025: A Comprehensive Comparison. Available at: https://www.optial.com/resources/top-grc-tools-2025 (accessed October 25 2025).
8. Malcolm, Gammisch, Signe, Balina (2014). The Effectiveness of Compliance Management Systems – An Experimental Approach. *Procedia – Social and Behavioral Sciences*, Volume 156, pp. 236–240. DOI: https://doi.org/10.1016/j.sbspro.2014.11.181
9. Ethics And Compliance Software Market Research Report 2033. *Dataintelo*: веб-сайт. Available at: https://dataintelo.com/report/ethics-and-compliance-software-market (accessed October 25 2025).
10. Lombardi, D. R., Vasarhelyi, M. A. ,Begg, I.(2014). Continuous Controls Monitoring: A Case Study. *Journal of Emerging Technologies in Accounting*. no. 11 (1). pp. 83–98. DOI: https://doi.org/10.2308/jeta-51006.
11. Eniola K., Okunola A., Gery, B. AI-driven regulatory technology (RegTech): Streamlining compliance and risk management in the financial sector [Manuscript]. *ResearchGate.* 2025. Available at: https://www.researchgate.net/publication/390450097. (accessed October 25 2025).
12. Chitraju Gopal Varma, Santhosh. The Future of AI-Enabled RegTech in U.S. Financial Markets. [Preprint]. *ResearchGate*. Available at: 10.13140/RG.2.2.30081.77929. (accessed October 25 2025).
13. What is RegTech and Why It Matters for Financial Services. *Codist.* Available at: https://www.codiste.com/what-is-regtech-guide-compliance-automation. (accessed October 25 2025).

Стаття надійшла: 03.11.2025
Стаття прийнята: 01.12.2025
Стаття опублікована: 26.12.2025