ФІНАНСИ, БАНКІВСЬКА СПРАВА, СТРАХУВАННЯ ТА ФОНДОВИЙ РИНОК

УДК 368:005.334:004.056
DOI: https://doi.org/10.32782/2415-3583/40.14

Борисюк О.В.
кандидат економічних наук, доцент
Волинський національний університет імені Лесі Українки
ORCID: https://orcid.org/ 0000-0002-9411-4118

Дацюк-Томчук М.Б.
кандидат економічних наук, доцент
Луцький інститут розвитку людини Університету «Україна»
ORCID: https://orcid.org/0000-0002-9794-8943

СИНТЕЗ КОМПЛАЄНСУ ТА КІБЕРБЕЗПЕКИ ЯК СТРАТЕГІЧНИЙ ВЕКТОР ЗМІЦНЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ СТРАХОВИКА

У статті досліджено теоретичні та прикладні аспекти забезпечення комплаєнсу та кібербезпеки в діяльності страхових компаній в умовах цифровізації фінансового сектору. Авторами розкрито взаємозв'язок між дотриманням нормативно-правових вимог та захистом інформаційних систем як фундаменту економічної безпеки страховика. Проведено порівняльний аналіз сутнісних характеристик комплаєнсу та кібербезпеки, визначено їхні ключові інструменти, серед яких виділено організаційні, технічні, правові та інноваційні засоби. Особливу увагу приділено ідентифікації ризиків (регуляторних, кібернетичних, операційних, фінансових), що безпосередньо впливають на стабільність фінансів страховика. Обґрунтовано роль міжнародних стандартів, таких як ISO/IEC 27001, GDPR та Solvency II, у мінімізації фінансових втрат та підвищенні довіри клієнтів. Визначено стратегічні напрями вдосконалення системи захисту через інвестування в кібертехнології та інтеграцію RegTech-рішень.

Ключові слова: *страхова компанія, фінанси страховика, безпека страховика, комплаєнс, кібербезпека, безпека фінансів страховика, економічна безпека страхових компаній.*

Постановка проблеми. Стрімка цифровізація страхового ринку підвищує ефективність бізнес-процесів, але одночасно створює критичні вразливості, пов'язані з витоком персональних даних, шахрайством та масштабними кібератаками. Питання захисту фінансів страховика та забезпечення його економічної безпеки стають неможливими без інтеграції системи внутрішнього контролю (комплаєнсу) та надійного технологічного захисту (кібербезпеки). Необхідність пошуку балансу між дотриманням жорстких регуляторних норм та впровадженням інноваційних методів протидії кіберризикам визначає актуальність дослідження механізмів стабілізації фінансового стану страхових компаній.

Аналіз останніх досліджень і публікацій. Питання забезпечення безпекових аспектів страхування як складного соціально-економічного явища постійно перебувають у центрі уваги провідних науковців. Дослідники активно аналізують механізми відшкодування збитків за рахунок фінансових ресурсів страховика, вивчають специфіку розподілу страхових ризиків, а також особливості формування та цільового використання страхових резервів.

Вагомий внесок на вплив поведінкових чинників на ефективність управління фінансовою діяльністю корпоративних структур та стратегічні перспективи розвитку національного ринку страхування висвітлено у працях як вітчизняних так і зарубіжних авторів, зокрема: О. В. Длугопольський [9], О. В. Золотарьова [2], К. М. Мельник [6], А. В. Нечипоренко [3], О. Т. Прокопчук [6], Д. О. Хропонюк [9], Ю. А. Цимбалюк [6], Н. О. Федорова [8], М. С. Федоренко [7], R. M. Snishchenko [10], L. N. Krot [10] та інших.

Попри значну кількість напрацювань, стрімка цифровізація фінансового сектору вимагає додаткового вивчення інтегрованого впливу кіберзагроз та регуляторного комплаєнсу на фінансову стабільність страховиків, що й зумовлює вибір теми даної статті.

Метою статті є узагальнення сутнісних характеристик комплаєнсу та кібербезпеки, ідентифікація ключових ризиків, що впливають на фінанси та безпеку страховика, а також систематизація інструментів і міжнародних стандартів, спрямованих на забезпечення ефективного функціонування страхових компаній у сучасному цифровому середовищі.

Виклад основного матеріалу дослідження. У сучасних умовах цифровізації фінансового сектору особливого значення набувають питання забезпечення комплаєнсу та кібербезпеки в діяльності страхових компаній. Страховий ринок активно інтегрує цифрові технології, що підвищує ефективність бізнес-процесів, але водночас створює нові ризики, пов'язані з витоком даних, шахрайством та кібератаками.

Комплаєнс виступає ключовим інструментом дотримання нормативно-правових вимог, тоді як кібербезпека забезпечує захист інформаційних систем та персональних даних клієнтів. Взаємодія цих двох складових формує основу економічної безпеки страховика.

Комплаєнс у страхових компаніях – це система внутрішнього контролю, спрямована на забезпечення відповідності діяльності вимогам законодавства, нормативних актів та внутрішніх політик [1, с. 87].

Кібербезпека – це сукупність заходів, спрямованих на захист інформаційних систем, мереж та даних від несанкціонованого доступу, пошкодження або знищення [2, с. 414].

Взаємозв'язок комплаєнсу та кібербезпеки проявляється у забезпеченні [3]:

– захисту персональних даних клієнтів;

– прозорості фінансових операцій;

– дотримання міжнародних стандартів (ISO, GDPR тощо).

З метою більш чіткого розуміння ролі комплаєнсу та кібербезпеки у забезпеченні ефективного функціонування страхових компаній доцільно узагальнити їх ключові характеристики та відмінності. Особливу увагу слід приділити їх впливу на фінанси страховика та рівень його економічної безпеки, оскільки саме ці складові формують основу стабільності та надійності страхової діяльності. Узагальнення сутнісних ознак комплаєнсу та кібербезпеки представлено в табл. 1.

Як видно з табл. 1 , комплаєнс і кібербезпека мають різну функціональну спрямованість, однак у сукупності забезпечують комплексний підхід до захисту діяльності страховика. Якщо комплаєнс орієнтований на дотримання нормативно-правових вимог та мінімізацію юридичних ризиків, то кібербезпека зосереджується на захисті інформаційних ресурсів і технологічної інфраструктури. Їх взаємодія сприяє підвищенню рівня безпеки фінансів страховика, зменшенню ризику фінансових втрат та формуванню довіри з боку клієнтів і регуляторів [6, с. 6].

У процесі функціонування страхових компаній виникає широкий спектр ризиків, які можуть суттєво впливати на фінанси страховика та рівень його економічної безпеки. Ідентифікація та систематизація таких ризиків є необхідною передумовою для побудови ефективної системи комплаєнсу та кіберзахисту. Узагальнену характеристику основних ризиків, що впливають на діяльність страховиків, наведено в табл. 2.

Як видно з табл. 2, найбільшу загрозу для фінансів страховика становлять кіберризики та регуляторні порушення, які можуть призвести до значних фінансових втрат і санкцій. Водночас операційні та репутаційні ризики мають опосередкований, але не менш

Таблиця 1 – Сутність комплаєнсу та кібербезпеки в діяльності страховиків

Критерій	Комплаєнс	Кібербезпека
Сутність	Дотримання норм і правил	Захист інформаційних систем
Основна мета	Мінімізація правових ризиків	Запобігання кібератакам
Об'єкт контролю	Бізнес-процеси	IT-інфраструктура
Інструменти	Політики, аудит, контроль	Антивірус, шифрування, IDS
Результат	Законність діяльності	Безпека даних

Джерело: складено за [4; 6; 7]

Таблиця 2 – Основні ризики комплаєнсу та кібербезпеки страховиків

Група ризиків	Характеристика	Причини виникнення	Вплив на фінанси страховика	Вплив на безпеку старховика
Регуляторні	Порушення законодавства та нормативних вимог	Недосконалість внутрішнього контролю, зміни законодавства	Штрафи, санкції, фінансові втрати	Зниження рівня правової безпеки
Операційні	Помилки персоналу, недоліки процесів	Низька кваліфікація, людський фактор	Непрямі фінансові втрати	Порушення внутрішньої безпеки
Кіберризики	Хакерські атаки, віруси, фішинг	Низький рівень IT-захисту, цифровізація	Прямі фінансові втрати, витік коштів	Порушення інформаційної безпеки
Репутаційні	Втрата довіри клієнтів і партнерів	Порушення безпеки, скандали	Зменшення доходів, відтік клієнтів	Підрив довіри до компанії
Технологічні	Збої IT-систем, технічні несправності	Застаріле обладнання, відсутність оновлень	Переривання фінансових операцій	Зниження технічної безпеки
Фінансові	Неефективне управління фінансовими ресурсами	Помилки у фінансовому плануванні	Зниження прибутковості, збитки	Ослаблення фінансової безпеки
Шахрайські	Внутрішнє та зовнішнє шахрайство	Недостатній контроль, цифрові загрози	Прямі фінансові втрати	Порушення комплексної безпеки
Стратегічні	Неправильні управлінські рішення	Недостатній аналіз ризиків	Довгострокові фінансові втрати	Зниження загальної безпеки

Джерело: складено за [4; 6; 7; 10]

важливий вплив на рівень безпеки діяльності страхової компанії. Це обумовлює необхідність комплексного підходу до управління ризиками [7, с. 22].

Забезпечення належного рівня безпеки фінансів страховика потребує використання комплексу інструментів, що охоплюють організаційні, технічні, правові та контрольні аспекти діяльності. Ефективне поєднання інструментів комплаєнсу та кібербезпеки дозволяє мінімізувати ризики та підвищити стійкість страхової компанії до внутрішніх і зовнішніх загроз [8]. Основні інструменти забезпечення безпеки систематизовано в табл. 3.

Дані табл. 3 свідчать про те, що ефективне управління фінансами страховика неможливе без інтеграції комплаєнс-процедур та сучасних технологій кіберзахисту. Використання таких інструментів, як внутрішній аудит, моніторинг операцій і системи інформаційної безпеки, сприяє підвищенню рівня безпеки та зменшенню ймовірності фінансових втрат [9, с. 120].

В умовах глобалізації та цифровізації страхового ринку особливого значення набуває впровадження міжнародних стандартів, які забезпечують високий рівень безпеки фінансів страховика та уніфікацію підходів до управління ризиками. Такі стандарти сприяють підвищенню прозорості діяльності страхових компаній та зміцненню довіри з боку клієнтів і регуляторів. Основні міжнародні стандарти у сфері комплаєнсу та кібербезпеки наведено в табл. 4.

Як видно з табл. 4 , міжнародні стандарти відіграють ключову роль у забезпеченні безпеки діяльності страхових компаній та захисту їх фінансових ресурсів. Їх впровадження дозволяє підвищити ефективність управління фінансами страховика, мінімізувати ризики та забезпечити відповідність сучасним вимогам цифрової економіки.

Таблиця 3 – Інструменти забезпечення комплаєнсу та кібербезпеки

Напрям	Інструменти комплаєнсу	Інструменти кібербезпеки	Вплив на фінанси страховика	Вплив на безпеку страховика
Організаційний	Кодекс етики, комплаєнс-політики, внутрішні регламенти	Навчання персоналу, політики інформаційної безпеки	Зниження ризику штрафів і санкцій	Підвищення рівня внутрішнього контролю
Технічний	Системи моніторингу операцій, автоматизація контролю	Firewall, антивірус, шифрування, IDS/IPS	Запобігання фінансовим втратам від кібератак	Захист інформаційних ресурсів
Правовий	Внутрішні нормативні документи, комплаєнс-контроль	Захист персональних даних, юридичне регулювання IT	Уникнення фінансових санкцій	Забезпечення правової безпеки
Контрольний	Внутрішній аудит, комплаєнс-перевірки	SIEM-системи, моніторинг інцидентів	Оптимізація фінансових втрат	Постійний контроль безпеки
Фінансовий	Аналіз фінансів страховика, фінансовий моніторинг	Захист платіжних систем, antifraud-системи	Забезпечення стабільності доходів	Захист від шахрайства
Інноваційний	RegTech-рішення, автоматизація комплаєнсу	AI/ML для виявлення загроз, Big Data-аналітика	Оптимізація витрат і підвищення ефективності	Проактивний захист

Джерело: складено за [5; 6; 7; 10]

Таблиця 4 – Міжнародні стандарти у сфері комплаєнсу та кібербезпеки страховиків

Стандарт	Сфера застосування	Ключові вимоги	Вплив на фінанси страховика	Вплив на безпеку страховика
ISO/IEC 27001	Інформаційна безпека	Впровадження системи управління інформаційною безпекою (ISMS)	Зниження фінансових втрат від витоку даних	Захист інформаційних активів
GDPR	Захист персональних даних	Обробка даних за згодою, право на захист і видалення	Уникнення штрафів та санкцій	Захист персональних даних клієнтів
Solvency II	Регулювання страхового ринку	Вимоги до капіталу, управління ризиками	Підвищення фінансової стійкості	Комплексна економічна безпека
NIST Cybersecurity Framework	Кібербезпека	Ідентифікація, захист, виявлення, реагування	Мінімізація кіберфінансових ризиків	Системний кіберзахист
ISO 22301	Управління безперервністю бізнесу	Планування безперервності діяльності (BCP)	Зменшення втрат від простоїв	Стійкість до кризових ситуацій
PCI DSS	Безпека платіжних операцій	Захист платіжних даних клієнтів	Запобігання фінансовому шахрайству	Безпека транзакцій
COBIT	IT-управління та контроль	Управління IT-процесами та ризиками	Оптимізація витрат на IT	Контроль IT-ризиків
ISO 31000	Управління ризиками	Ідентифікація, оцінка та управління ризиками	Зменшення фінансових ризиків	Загальна система безпеки

Джерело: складено за [5; 6; 7; 10]

Водночас, для підвищення рівня безпеки страхових компаній доцільно [10, с. 70]:

– впроваджувати цифрові технології контролю (RegTech, SupTech);

– підвищувати кваліфікацію персоналу;

– посилювати державне регулювання;

– інтегрувати системи управління ризиками;

– інвестувати в кіберзахист.

Комплаєнс та кібербезпека є взаємопов'язаними елементами системи економічної безпеки страхових компаній. В умовах цифровізації їх роль значно зростає, оскільки саме вони забезпечують довіру клієнтів, стабільність функціонування та відповідність нормативним вимогам, а ефективне управління комплаєнсом і кіберризиками дозволяє мінімізувати загрози, підвищити конкурентоспроможність страховика та сприяти сталому розвитку страхового ринку.

Висновки. Узагальнюючи результати дослідження, можна констатувати, що в умовах цифровізації страхового ринку комплаєнс та кібербезпека є взаємопов'язаними елементами системи економічної безпеки, які забезпечують стабільність функціонування та довіру клієнтів. Хоча ці напрями мають різну функціональну спрямованість – дотримання норм і правил проти захисту інформаційних систем – їх синергія дозволяє ефективно мінімізувати регуляторні, операційні та кіберризики, які становлять найбільшу загрозу для фінансів страховика. Використання комплексних інструментів, таких як моніторинг операцій, антифрод-системи та впровадження міжнародних стандартів (ISO/IEC 27001, GDPR, Solvency II), сприяє підвищенню фінансової стійкості та захисту активів від зовнішніх і внутрішніх загроз. Таким чином, інтеграція сучасних технологій кіберзахисту та суворих процедур комплаєнс-контролю є стратегічно необхідною умовою для забезпечення конкурентоспроможності та сталого розвитку страхових компаній у сучасному цифровому середовищі.

Список використаних джерел:

1. Борисюк О. В., Ткачук Н. В. Моніторинг бізнес-процесів страховиків в умовах цифровізації. *Економіка, фінанси, право.* № 10. 2024. с. 84–88. DOI: https://doi.org/10.37634/efp.2024.10.18

2. Золотарьова О. В. Ключові тенденції та пріоритети розвитку ринку страхових послуг в Україні. *Економіка і суспільство.* 2017. № 11. С. 413–420.

3. Нечипоренко А. В. Державне регулювання страхової діяльності в Україні: теоретичний аспект. *Ефективна економіка.* 2021. № 7. URL: http://www.economy.nayka.com.ua/pdf/7_2021/96.pdf

4. Огляд небанківського фінансового сектору за 2025 рік. *Національний банк України.* URL: https://bank.gov.ua/admin_uploads/article/Nonbanking_Sector_Review_2025-11.pdf?v=15

5. Показники діяльності страховиків. Наглядова статистика. *Національний банк України.* URL: https://bank.gov.ua/ua/statistic/supervision-statist

6. Прокопчук О., Цимбалюк Ю. А., Мельник К. М. Інвестиційна діяльність страхових організацій в Україні. *Інвестиції: практика та досвід.* 2021. № 16. С. 5–12. DOI: https://doi.org/10.32702/23066814.2021.16.5

7. Федоренко М.С. Інвестиційна діяльність страхових компаній в Україні. *Інвестиції: практика та досвід*. 2013. № 9. С. 21–23.

8. Федорова Н.О. Державне регулювання напрямків страхової діяльності в Україні. *Публічне адміністрування та національна безпека.* 2019. № 1. DOI: https://doi.org/10.25313/2617-572X-2019-1-4856

9. Хропонюк Д. О., Длугопольський О. В. Сучасні проблеми та перспективи розвитку страхового ринку України. *Innovation and Sustainability.* 2023. № 1. С. 118–126. DOI: https://doi.org/10.31649/ins.2023.1.118.126

10. Snishchenko R., Krot L. Features of the work organization of insurance companies of Ukraine during the period of armed. *Трансформаційна економіка*. № 4 (04) 2023. С. 66–71. DOI: https://doi.org/10.32782/2786-8141/2023-4-12

References:

1. Borysiuk, O. V., & Tkachuk, N. V. (2024). Monitorynh biznes-protsesiv strakhovykiv v umovakh tsyfrovizatsii [Monitoring of business processes of insurers in the conditions of digitalization]. *Ekonomika, finansy, pravo*, no. 10, pp. 84–88. DOI: https://doi.org/10.37634/efp.2024.10.18

2. Zolotariova, O. V. (2017). Kliuchovi tendentsii ta priorytety rozvytku rynku strakhovykh posluh v Ukraini [Key trends and priorities of insurance market development in Ukraine]. *Ekonomika i suspilstvo,* no.11, pp. 413–420.

3. Nechyporenko, A. V. (2021). Derzhavne rehuliuvannia strakhovoi diialnosti v Ukraini: teoretychnyi aspekt [State regulation of insurance activity in Ukraine: theoretical aspect]. *Efektyvna ekonomika*, no 7. Available at: http://www.economy.nayka.com.ua/pdf/7_2021/96.pdf.

4. National Bank of Ukraine. (2025). *Ohliad nebankivskoho finansovoho sektoru za 2025 rik* [Non-banking sector review for 2025]. Available at: https://bank.gov.ua/admin_uploads/article/Nonbanking_Sector_Review_2025-11.pdf?v=15

5. National Bank of Ukraine. *Pokaznyky diialnosti strakhovykiv. Nahliadova statystyka* [Insurers' performance indicators. Supervisory statistics]. Available at: https://bank.gov.ua/ua/statistic/supervision-statist

6. Prokopchuk, O. T., Tsymbaliuk, Yu. A., & Melnyk, K. M. (2021). Investytsiina diialnist strakhovykh orhanizatsii v Ukraini [Investment activity of insurance organizations in Ukraine]. *Investytsii: praktyka ta dosvid*, no. (16), pp. 5–12. DOI: https://doi.org/10.32702/23066814.2021.16.5

7. Fedorenko, M. S. (2013). Investytsiina diialnist strakhovykh kompanii v Ukraini [Investment activity of insurance companies in Ukraine]. *Investytsii: praktyka ta dosvid*, no. 9, pp. 21–23.

8. Fedorova N.O. (2019). Derzhavne rehuliuvannia napriamkiv strakhovoi diialnosti v Ukraini [State regulation of insurance activities in Ukraine]/ Publichne administruvannia ta natsionalna bezpeka., no. 1. DOI: https://doi.org/10.25313/2617-572X-2019-1-4856

9. Khroponiuk, D. O., Dluhopolskyi, O. V. (2023). Suchasni problemy ta perspektyvy rozvytku strakhovoho rynku Ukrainy [Modern problems and perspectives of the development of the insurance market of Ukraine]. *Innovation and Sustainability*, no.1, pp. 118–126. DOI: https://doi.org/10.31649/ins.2023.1.118.126

10. Snishchenko, R., & Krot, L. (2023). Features of the work organization of insurance companies of Ukraine during the period of armed conflict. *Transformational Economy*, no.4, pp. 66–71. DOI: https://doi.org/10.32782/2786-8141/2023-4-12

Borysiuk Olena
Lesya Ukrainka Volyn National University
Datsyuk-Tomchuk Maria
Lutsk Institute of Human Development University "Ukraine"

SYNTHESIS OF COMPLIANCE AND CYBERSECURITY AS A STRATEGIC VECTOR OF STRENGTHENING THE ECONOMIC SECURITY OF THE INSURER

The article thoroughly examines the theoretical, methodological and practical principles of ensuring compliance and cybersecurity in the activities of insurance companies in the context of the rapid digitalization of the modern financial sector. The authors prove that the active integration of digital technologies into the insurance market, although it increases the efficiency of business processes, at the same time generates new specific risks, in particular the threats of confidential data leakage, financial fraud and large-scale cyberattacks. The paper substantiates that compliance in insurance companies acts as a multi-level internal control system that guarantees the compliance of the institution's activities with legislative norms and internal policies. In parallel, cybersecurity is considered as a critical set of measures to protect information networks and databases from unauthorized interference or destruction. Particular attention is paid to the synergistic effect of the interaction of these two components, which form the foundation of the insurer's economic security. The authors systematized the key characteristics of compliance and cybersecurity, highlighting their differences in control objects and tools, but emphasizing the single goal - ensuring the legality and security of data. The study identified a wide range of risks, where the most critical impact on the insurer's finances is regulatory and cyber risks, which can lead to direct monetary losses, asset leakage or loss of license. An important aspect of the article is the analysis of the role of international standards (ISO/IEC 27001, GDPR, Solvency II, NIST) in harmonizing the domestic insurance market with European requirements. The implementation of these standards is defined as a strategic step to strengthen the trust of customers and regulators and ensure the continuity of insurance services in crisis situations. In the final part of the work, a set of strategic recommendations is proposed to increase the level of security of insurers, which includes investing in modern cyber protection, automation of compliance procedures and continuous training of personnel. The study results emphasize that only an integrated approach to compliance and cyber threat management allows insurance companies to remain competitive and ensure sustainable development in the digital economy.

Keywords: *insurance company, insurer finances, insurer security, compliance, cybersecurity, insurer financial security, economic security of insurance companies.*

JEL Classification: G22, G32, M48, O33

Дата надходження статті: 17.02.2026
Дата прийняття статті: 10.03.2026
Дата публікації статті: 29.05.2026