

2. Загарій В.К., Синільник В.В. Особливості інноваційного потенціалу підприємств паливно-енергетичної галузі України. *«Економіка і суспільство»*. 2018. №14. С.182-187.

3. Замула І., Шавурська О., Кірейцева Г. Сталий розвиток України як інноваційний підхід до її післявоєнного відновлення. *Наука та інновації*, 2024. №20 (3), С.3–16.

УДК 330.131.7:368:004.9

Губа В. Р., аспірант,
Івано-Франківський національний технічний університет нафти і газу
Король С. В., к.е.н., доцент кафедри
фінансів, обліку та оподаткування,
Івано-Франківський національний технічний університет нафти і газу

ВПЛИВ ЦИФРОВІЗАЦІЇ НА СИСТЕМУ РИЗИК-МЕНЕДЖМЕНТУ СТРАХОВИХ КОМПАНІЙ

Цифровізація стала визначальним фактором розвитку фінансового сектору, зокрема страхових компаній. В умовах мінливого середовища впровадження цифрових технологій здатне сприяти підвищенню ефективності страхового бізнесу. Водночас воно створює нові виклики, які пов'язані з кібербезпекою, регуляторними змінами, технологічними інноваціями та трансформацією споживчих звичок. Відтак ризик-менеджмент у страхових компаніях у контексті цифровізації набуває стратегічного значення, оскільки дозволяє зменшити вплив цифрових загроз та адаптувати бізнес-моделі до змін ринкового середовища.

У площині страхового сектору можемо виокремити такі ключові ризики цифровізації, як кібербезпека та захист інформаційних систем [1-3].

Власне, страхові компанії обробляють великі обсяги конфіденційної фінансової та персональної інформації, що робить їх особливо вразливими до кібератак. Тому підвищення захищеності цифрових платформ та розробка механізмів кібербезпеки є необхідною умовою стабільного функціонування страхових компаній. Відтак з метою забезпечення кібербезпеки можна запропонувати такі основні заходи як: використання багатофакторної автентифікації для захисту клієнтських даних; запровадження систем моніторингу та реагування на кіберзагрози; проведення періодичного аудиту безпеки інформаційних ресурсів.

Прикладом багатофакторної автентифікації (MFA) є Google та Microsoft Authenticator, – популярні програми для генерації кодів MFA, що використовуються у фінансових установах. Також можна навести банківські системи, так як більшість європейських банків запровадили MFA для входу в онлайн-банкінг, що значно зменшило кількість шахрайських атак. Прикладом є і корпоративні мережі, оскільки компанії впроваджують біометричну

автентифікацію (відбитки пальців, розпізнавання обличчя) для захисту доступу до критичних даних.

Серед систем моніторингу та реагування на кіберзагрози можемо виділити: Національний центр резервування державних інформаційних ресурсів, який використовує IDS/IPS-системи для виявлення та блокування атак на державні інформаційні ресурси; Microsoft Defender MDR – кероване виявлення та реагування на загрози, що дозволяє компаніям оперативно нейтралізувати кібератаки; SIEM-системи – великі корпорації застосовують Splunk, IBM QRadar для аналізу мережевого трафіку та виявлення аномалій [1-3].

Прикладом аудиту безпеки інформаційних ресурсів є: ISO 27001 сертифікація – міжнародний стандарт, який вимагає регулярного аудиту безпеки для фінансових установ; фінансові компанії, у яких щорічний аудит кібербезпеки проводиться для відповідності вимогам Національного банку України; внутрішній аудит, де компанії впроваджують регулярні перевірки безпеки, щоб виявити слабкі місця та запобігти витоку даних.

Також серед ключових ризиків цифровізації можемо виокремити аналіз даних та прогнозування ризиків [1-3]. Власне, цифровізація дозволяє страховим компаніям використовувати великі масиви даних, що сприяє точнішому визначенню ризиків, персоналізації страхових продуктів та вдосконаленню механізмів управління ризиками. У цьому процесі доцільно виокремити досить важливі аспекти аналітики великих даних, серед яких: використання штучного інтелекту для аналізу поведінкових моделей клієнтів; впровадження автоматизованих алгоритмів для визначення рівня ризиків; оптимізація страхових тарифів відповідно до актуальної аналітики.

Наочним прикладом аналізу даних та прогнозування ризиків є страхова компанія Swiss Re, яка, власне, впроваджує штучний інтелект та машинне навчання для аналізу ризиків у страхуванні; застосовує аналітичні алгоритми для покращення моделювання ризиків, прогнозування страхових випадків та персоналізації страхових продуктів; AI-інструменти дозволяють знижувати страхові витрати та підвищувати точність оцінки ризиків.

Вищезазначене свідчить про те, що цифрові технології мають значний вплив на управління ризиками. Перш за все, зростання цифровізації призводить до змін у страховій сфері шляхом впровадження блокчейн-технологій, Інтернету речей (IoT), машинного навчання та інших інновацій. Однак, зміни в законодавстві, пов'язані з цифровізацією, вимагають постійного моніторингу та адаптації до нових стандартів кібербезпеки та захисту персональних даних. Відтак в умовах мінливого середовища мають місце головні виклики технологічної трансформації, серед яких: недостатня перевірка алгоритмів перед їх комерційним застосуванням; вразливість цифрових платформ до технічних збоїв та помилок; недовіра клієнтів до автоматизованих страхових сервісів без людського контролю [1-3].

Загалом, в умовах сучасних викликів цифровізація страхового бізнесу кардинально змінює підходи до ризик-менеджменту, що створює нові виклики та можливості. Зокрема, кібербезпека стала ключовим напрямом

ризик-менеджменту; аналітика великих даних дозволяє точніше прогнозувати ризики та запобігати шахрайству; впровадження нових технологій формує ризики технічних збоїв, що потребує ретельного тестування; регуляторне середовище трансформується, що змушує страхові компанії адаптуватися до нових цифрових стандартів. Відтак грамотно вибудована система ризик-менеджменту здатна дозволити страховим компаніям мінімізувати загрози цифровізації та забезпечити стабільність бізнес-моделі у швидкозмінному технологічному середовищі.

Перелік використаних джерел

1. European Insurance and Occupational Pensions Authority (EIOPA). *Digitalisation and cybersecurity in the insurance sector*. 2023. URL: https://www.eiopa.europa.eu/index_en
2. Swiss Re Group. *The impact of digitalisation on insurance risk management*. 2021. URL: <https://www.swissre.com>
3. Tomašević V., Tomasevic M. Insurance market after COVID-19. Insurance issues regarding cyber security threats. In book: J.Kočović et al. (Eds.). Chapter: 23. Publisher: University of Belgrade - Faculty of Economics. 2020, pp.421-440. URL: https://www.researchgate.net/publication/359820789_Insurance_issues_regarding_cyber_security_threats

УДК 352:(005.21:332)

Данилюк М.О., доктор економічних наук, професор,
голова циклової комісії спеціальності 051 Економіка Відокремленого
структурного підрозділу «Бурштинський енергетичний фаховий коледж
Івано-Франківського національного технічного університету нафти і газу»,
Барабалюк Р.С., завідувачка економічного відділення
Відокремленого структурного підрозділу
«Бурштинський енергетичний фаховий коледж
Івано-Франківського національного технічного університету нафти і газу»,
Ковальський Т.А., голова циклової комісії економічних
дисциплін Відокремленого структурного підрозділу
«Бурштинський енергетичний фаховий коледж
Івано-Франківського національного технічного університету нафти і газу».

ПРО ВЗАЄМОЗВ'ЯЗОК СТРАТЕГІЧНИХ ДОКУМЕНТІВ З РОЗВИТКУ ТЕРИТОРІАЛЬНИХ ГРОМАД В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

Намічені орієнтири децентралізації та розбудови місцевого самоврядування в Україні посилюють актуальність стратегічного планування розвитку територіальних громад. Їхня діяльність повинна бути адекватна