

Таким чином, управлінський облік не лише є важливим інструментом фінансового менеджменту, а й сприяє підвищенню конкурентоспроможності підприємства в довгостроковій перспективі.

Список використаних джерел:

1. Управлінський облік. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Управлінський_облік (дата звернення: 02.03.2025).
2. Сутність, завдання та функції управлінського обліку. *StudFiles*. URL: <https://studfile.net/preview/6490963/page:2/> (дата звернення: 02.03.2025).
3. Особливості та взаємозв'язок управлінського і фінансового аналізу - Облік і фінанси АПК: освітній портал. *Облік і фінанси АПК: освітній портал*. URL: <https://magazine.faaf.org.ua/osoblivosti-ta-vzaemozv-yazok-upravlinskogo-i-finansovogo-analizu.html> (дата звернення: 02.03.2025).

Abstract: *The study examines the essence of management accounting, its main characteristics and significance for the financial management of an enterprise. Management accounting methods are described, in particular cost analysis, budgeting, break-even analysis and the balanced scorecard system.*

Keywords: *management accounting, financial management, budgeting, costs, break-even analysis.*

Науковий керівник:

Мельник О.І.,

*кандидат економічних наук, доцент
кафедри фінансів, банківської справи та страхування
Миколаївський національний аграрний університет*

УДК 336.368

Світові тенденції розвитку кіберстрахування

Вікторія Сaitгарєєва,

здобувач вищої освіти спеціальності

072 Фінанси, банківська справа та страхування

Миколаївський національний аграрний університет

м. Миколаїв, Україна

Анотація: *розглянуто сучасні тенденції кіберстрахування у світі, висвітлено ключові фактори, що впливають на його розвиток. Обґрунтовано перспективні напрями його активного зростання.*

Ключові слова: *кіберстрахування, кібербезпека, кіберзагроза, кіберризики.*

У сучасному світі стрімкий розвиток інформаційних технологій та цифрових технологій створює нові можливості для бізнесу, урядів та громадян. Проте, зростання рівня цифровізації супроводжується збільшенням ризиків кіберзлочинності, що змушує компанії шукати ефективні механізми захисту від кіберзагроз. Одним із таких механізмів є кіберстрахування, яке стало важливим елементом управління ризиками у багатьох країнах світу.

Кіберстрахування – це вид страхування, який забезпечує фінансовий захист компаніям і приватним особам від втрат, пов'язаних з кібератаками, витоками

даних та іншими кіберінцидентами. Основними об'єктами кіберстрахування є: витрати на відновлення після кібератак; судові витрати та виплати за позовами; витрати на реагування на витоки даних; репутаційні втрати та фінансові збитки. Страховий договір зазвичай відшкодовує втрати, завдані кібератаками або спричинені знищенням даних, їхнім несанкціонованим викраденням. Також передбачено покриття зупинок у роботі підприємства та зменшення доходу, спричинених кіберзагрозами, а також відповідальності компанії перед сторонніми особами у випадку, якщо вона не змогла забезпечити належний захист інформації. Окрім цього, розширене страхування може містити аудит ІТ-безпеки клієнта після інциденту, витрати на розслідування випадку та заходи з управління репутацією [1].

Світовий ринок кіберстрахування розвивається під впливом низки факторів, серед яких:

- зростання кількості кібератак. За останні роки кількість кіберзлочинів суттєво зросла, що збільшило попит на страхування кіберризиків.
- посилення регуляторних вимог. Уряди багатьох країн приймають закони, які зобов'язують компанії дотримуватися жорстких стандартів кібербезпеки.
- розвиток цифрової економіки. Все більше компаній переходять на цифрові технології, що підвищує їхню вразливість до кіберзагроз.
- зростання усвідомлення ризиків. Багато компаній починають розуміти важливість управління кіберризиками та звертаються до страхових компаній.

Багато страховиків застосовують штучний інтелект для оцінки кіберризиків та вдосконалення моделей ціноутворення. Це дозволяє покращити точність оцінки ризиків і зменшити ймовірність шахрайства. Уряди та міжнародні організації запроваджують нові стандарти та вимоги до кіберстрахування, що сприяє зростанню прозорості ринку.

Раніше кіберстрахування в основному використовувалося великими корпораціями, проте сьогодні все більше малих та середніх підприємств розглядають можливість страхування кіберризиків [2].

Попри швидкий розвиток ринку, кіберстрахування стикається з низкою викликів. Наприклад, через динамічний характер кіберзагроз страховим компаніям складно точно прогнозувати ризики та розраховувати страхові тарифи. Відсутність єдиних міжнародних стандартів ускладнює розвиток ринку кіберстрахування. Також, деякі компанії вважають кіберстрахування надто дорогим і не можуть собі його дозволити.

Очікується, що в найближчі роки ринок кіберстрахування продовжить активно зростати. Основними напрямками його розвитку стануть: розробка нових страхових продуктів, адаптованих до специфіки різних галузей; впровадження обов'язкового страхування кіберризиків у певних сферах (наприклад, у фінансовому секторі та охороні здоров'я); підвищення рівня кіберграмотності серед бізнесу та державних установ; співпраця страхових компаній з провайдерами кібербезпеки для зниження ризиків.

Отже, кіберстрахування відіграє важливу роль у сучасній цифровій економіці, забезпечуючи фінансовий захист компаніям від кіберзагроз.

Незважаючи на низку викликів, цей ринок має значний потенціал для подальшого зростання. Важливими завданнями для страховиків та урядів є покращення методів оцінки кіберризиків, зниження вартості страхових полісів та підвищення рівня кібербезпеки в усьому світі. В майбутньому кіберстрахування стане невід'ємною частиною стратегії управління ризиками для більшості компаній та організацій.

Список використаних джерел

1. Страхування кібер-ризиків. *Cyber insurance*. URL: <https://forinsurer.com/theme/48>.
2. Пікус Р. В., Бабенко Л. Ю. Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава – наукове фахове видання України з питань економіки*. 2022. URL: http://www.economy.in.ua/pdf/2_2022/25.pdf

Abstract: *reviewed current trends in cyber insurance in the world, highlighted key factors influencing its development. Prospective directions of its active growth are substantiated.*

Key words: *cyber insurance, cybersecurity, cyber threat, cyber risks.*

Науковий керівник:

Мельник О. І.,
кандидат економічних наук, доцент кафедри фінансів,
банківської справи та страхування,
Миколаївський національний аграрний університет

УДК 657.4:657.6

Ідентифікація та оцінка ризиків в управлінському обліку

Тетяна Слободян,

Здобувач вищої освіти спеціальності 071 Облік і оподаткування
Миколаївський національний аграрний університет
м. Миколаїв, Україна

Анотація: *у дослідженні розглянуто основні методи ідентифікації та оцінки ризиків. Практичне застосування цих методів у контексті управлінського обліку дозволяє організаціям розробляти ефективні стратегії для зменшення ризиків і підвищення фінансової стабільності.*

Ключові слова: *управлінський облік, ідентифікація ризиків, оцінка ризиків, аналіз сценаріїв, діаграма Ішिकाви, метод Дельфі, стратегічне управління.*

Ідентифікація та оцінка ризиків є ключовими складовими управлінського обліку, оскільки вони дозволяють організаціям передбачати потенційні загрози та приймати обґрунтовані рішення для їх мінімізації. У сучасному