

АУДИТ КІБЕРЗАХИСТУ В СТРУКТУРІ ОБЛІКОВОЇ ПОЛІТИКИ ПІДПРИЄМСТВА

БЛАНАР-ДУБІНІНА Поліна,
здобувач фахової передвищої освіти
ВСП «Технологіко-економічний коледж»
Миколаївського національного аграрного університету

Анотація: Досліджено роль аудиту кіберзахисту в системі облікової політики підприємства та його значення для забезпечення інформаційної безпеки. Визначено основні напрями аудиту, що охоплюють технічні, організаційні та кадрові аспекти захисту облікових даних. Наголошено, що системне впровадження аудиту кіберзахисту підвищує прозорість, надійність і конкурентоспроможність підприємства в умовах цифрової економіки.

Ключові слова: аудит, кіберзахист, облікова політика, інформаційна безпека, ризики, управління.

Актуальність аудиту кіберзахисту у сфері обліку визначається зростанням цифрових загроз та ускладненням технологічного середовища. Облікові дані перетворилися на стратегічний ресурс, від якого залежить фінансова стійкість і довіра користувачів до підприємства. Саме тому кіберзахист необхідно інтегрувати до системи облікової політики як складову її організаційного та методичного забезпечення.

Облікова політика розглядається не лише як набір методів ведення обліку, а й як механізм управління інформаційними ризиками. Включення положень щодо кіберзахисту в облікову політику сприяє підвищенню прозорості процесів та зміцненню довіри з боку інвесторів і контролюючих органів. Таким чином, політика підприємства виходить за межі суто бухгалтерського інструментарію і формує основу комплексної безпеки.

Аудит у цій площині виконує функцію незалежної перевірки. Він дозволяє оцінити відповідність заходів кіберзахисту ключовим принципам — конфіденційності, цілісності та доступності даних. Ці критерії визначають якість інформаційної системи і відображаються в міжнародних стандартах, що застосовуються у практиці обліку та аудиту.

У ході аудиту кіберзахисту виявляються типові слабкі місця. До них відносять відсутність систематичного резервного копіювання, нерегулярне оновлення програмного забезпечення, неналежний контроль за доступом до баз

даних. Усі ці фактори створюють передумови для втрати інформації або її несанкціонованої зміни. Нівелювання таких загроз потребує комплексного підходу до організації безпеки .

Особливе значення має оцінка кадрового чинника. Дослідження свідчать, що брак цифрової грамотності бухгалтерів і фінансових менеджерів істотно знижує ефективність захисту даних. Аудит у цій сфері має визначати рівень готовності персоналу дотримуватися вимог інформаційної безпеки, а також формувати рекомендації щодо навчання і внутрішніх інструкцій .

Регулярність проведення аудиту кіберзахисту доцільно закріпити в обліковій політиці підприємства. Це забезпечує сталість процесів контролю і сприяє адаптації системи до нових технологічних викликів. Системний характер перевірок дозволяє підтримувати необхідний рівень захищеності даних у динамічному цифровому середовищі .

Водночас аудит кіберзахисту не варто розглядати як разову процедуру. Він повинен мати превентивний характер і виконувати функцію моніторингу. Йдеться про виявлення потенційних ризиків ще до їх фактичної реалізації, що істотно знижує наслідки атак або технічних збоїв. Саме така профілактична роль аудиту робить його цінним для системи управління .

Наукові підходи підкреслюють необхідність поєднання технічних і організаційних аспектів аудиту. Технічні інструменти охоплюють аналіз програмних засобів захисту, тоді як організаційні — оцінку регламентів, політик і внутрішнього контролю. Синергія цих елементів формує більш цілісну систему перевірки, здатну ефективно реагувати на виклики цифрової економіки .

Сучасна практика свідчить, що аудит кіберзахисту в обліковій політиці потребує інтеграції з правовими нормами. Наявність у законодавстві вимог щодо збереження комерційної та фінансової таємниці вимагає від підприємств чіткої відповідальності за організацію захисту. Таким чином, аудит виконує і функцію перевірки правової відповідності .

Розширення сфери аудиту кіберзахисту сприяє появі нових професійних компетенцій бухгалтерів та аудиторів. Вони повинні володіти не лише

обліковими знаннями, а й розумінням основ кібербезпеки. Це вимагає вдосконалення освітніх програм і підвищення кваліфікації фахівців, які працюють з обліковою інформацією .

Інтеграція положень аудиту кіберзахисту в облікову політику створює основу для сталого розвитку підприємства. Забезпечення достовірності інформаційних потоків і захищеності даних є умовою ефективного стратегічного управління. Це особливо актуально в умовах глобальної конкуренції та швидкого технологічного прогресу .

Підсумовуючи, слід наголосити, що аудит кіберзахисту в структурі облікової політики виступає не лише механізмом контролю, а й інструментом вдосконалення системи управління. Його значення зростає у зв'язку з необхідністю забезпечення балансу між прозорістю обліку та захищеністю інформації. Впровадження системного аудиту дає змогу підприємствам підвищувати стійкість і формувати конкурентні переваги у цифровій економіці.

Література:

1. Цаль-Цалко Ю.С., Мороз Ю.Ю. Облікова політика підприємства та її кібербезпека // *Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства: збірник наукових праць*, том IV, частина I, Житомир: ПП «Рута», 2017 С. 8-11.

2. Муравський В. Облік та кібербезпека : монографія. Тернопіль : ЗУНУ, 2023. 200 с.

Abstract: The study examines the role of cybersecurity audit in the accounting policy system of an enterprise and its importance for ensuring information security. The main areas of audit are identified, covering technical, organizational, and human resource aspects of accounting data protection. It is emphasized that the systematic implementation of cybersecurity audit enhances the transparency, reliability, and competitiveness of an enterprise in the digital economy.

Keywords: audit, cybersecurity, accounting policy, information security, risks, management.

***Науковий керівник – ДУБІНІНА Марина,
д-р екон. наук, професор, завідувач кафедри обліку і оподаткування,
Миколаївський національний аграрний університет,
м. Миколаїв***