

спрямована на підтримку освітньої галузі, стане запорукою сталого розвитку економіки та забезпечення конкурентоспроможності українських фахівців на світовому ринку праці.

Перелік використаної літератури:

1. Гусейнов С., Гарань Н., Колесник К. ВИКЛИКИ ТА ПЕРСПЕКТИВИ ОСВІТИ УКРАЇНИ В УМОВАХ ВІЙНИ ТА У ПІСЛЯВОЄННИЙ ПЕРІОД. SCIENTIFIC PRACTICE: MODERN AND CLASSICAL RESEARCH METHODS. 2023. URL: <https://doi.org/10.36074/logos-26.05.2023.077>

Дубініна М.В.

д.е.н., професор

Чебан Ю.Ю.

к.е.н., доцент

Миколаївський національний аграрний університет

ФОРМУВАННЯ КІБЕРБЕЗПЕКОВИХ РЕГЛАМЕНТІВ ЯК ІНСТРУМЕНТУ ЗАХИСТУ ОБЛІКОВОЇ ІНФОРМАЦІЇ ПІДПРИЄМСТВ

Кібербезпека сучасного підприємства є невід'ємною складовою його стабільного функціонування в умовах глобальної цифровізації економіки. Однією з ключових передумов досягнення високого рівня кіберзахисту є створення та впровадження кібербезпекових регламентів облікової політики. Облікова політика виступає основоположним документом, який забезпечує регулювання внутрішніх інформаційних потоків і взаємодії з зовнішніми суб'єктами господарювання. Її вдосконалення з урахуванням кібербезпекових вимог дозволяє запобігти багатьом загрозам і сформувати комплексну систему захисту облікової інформації.

Дослідження взаємозв'язку між обліковою політикою та забезпеченням кібербезпеки підприємств є актуальною темою в науковій літературі. Так, Цаль-Цалко Ю.С. та Мороз Ю.Ю. розглядають кібербезпеку як цілісну систему захисту інформаційних ресурсів підприємства від потенційних внутрішніх і зовнішніх загроз, що базується на поєднанні організаційних, технічних та правових заходів [1]. У свою чергу, Герасимович І.А. запропонував концептуальну модель облікової політики, яка враховує різноманітні аспекти регулювання та об'єкти облікової діяльності, створюючи основу для інтеграції кібербезпекових елементів [2].

Вагомий внесок зробили також інші дослідники, зокрема Кафка С., яка наголошує на необхідності підпорядкування внутрішніх регламентів, таких як графіки документообігу та проекти автоматизації обліку, загальним принципам облікової політики [3]. Лоханова Н.О. у своєму дослідженні наголошує на багатофункціональності облікової політики як інструмента управління економічною безпекою підприємств, підкреслюючи її значення для забезпечення достовірності інформації у фінансовій, податковій та управлінській звітності [4]. Вона зазначає, що коректно розроблена облікова політика сприяє не лише зниженню ризиків та оптимізації податкових платежів, але й створює передумови для економічної стійкості шляхом страхування підприємства від фінансових втрат та рівномірного розподілу витрат. У цьому контексті обґрунтування Лоханової Н.О. щодо впливу вибору конкретних методів обліку на фінансові результати підприємства є надзвичайно важливим для формування кібербезпекових регламентів. Ці регламенти повинні інтегрувати не лише інформаційні, але й захисні аспекти, орієнтуючись на принципи об'єктивності, релевантності та безпеки даних, що є основою організаційного кіберзахисту. Аналіз літературних джерел дозволяє виділити ще одну важливу тенденцію: інтеграція кібербезпекових аспектів у внутрішні регламенти підприємства, такі як графіки документообігу та проекти автоматизації обліку. На думку фахівців, це не лише підвищує гнучкість і адаптивність системи обліку, але й створює передумови для довгострокової економічної стійкості підприємств.

Водночас організаційні аспекти кібербезпеки залишаються малодослідженими. Більшість робіт зосереджена на технічних питаннях, таких як програмне забезпечення та технологічні інструменти, залишаючи поза увагою регламентацію дій персоналу, контроль доступу до даних та створення безпечного середовища для роботи з обліковою інформацією. Ця ситуація вказує на

необхідність більш системного підходу до розробки безпекових регламентів, що поєднують організаційні й технічні аспекти захисту.

Розробка кібербезпекових регламентів облікової політики має ґрунтуватися на комплексному аналізі кіберризиків, характерних для сучасного бізнес-середовища. Підприємства стикаються з багатогранними загрозами, які охоплюють технічні, організаційні та інформаційні аспекти. Це вимагає врахування особливостей їхньої структури, масштабів діяльності та використовуваних технологій. Такий підхід забезпечує індивідуалізацію заходів безпеки та їх адаптацію до потреб конкретної організації.

Одним із центральних елементів кібербезпекових регламентів є впровадження чіткої системи ієрархічного доступу до інформаційних ресурсів підприємства. Це дозволяє обмежити доступ до конфіденційних даних лише тим працівникам, чия діяльність безпосередньо пов'язана з їх обробкою. Такий підхід значно зменшує ризик витоку інформації через помилки чи недбалість персоналу, що, як відомо, є однією з найпоширеніших причин порушення безпеки.

Для підвищення рівня автентифікації персоналу доцільно використовувати персоналізовані цифрові підписи. Ці інструменти не лише забезпечують точне ідентифікування користувачів, але й дозволяють фіксувати всі їхні дії в інформаційному середовищі. Таким чином, підприємство отримує можливість оперативно виявляти потенційні загрози та нейтралізувати їх до того, як вони переростуть у серйозні проблеми.

Особливу увагу слід приділяти розподілу прав доступу залежно від рівня відповідальності співробітників. Для працівників нижчих ієрархічних рівнів доцільно обмежити доступ до мінімального набору даних, необхідного для виконання їхніх завдань, тоді як для керівників чи фахівців із стратегічних питань обсяг доступу має бути ширшим, що сприяє ефективному вирішенню складних управлінських завдань.

Також важливо впроваджувати стандартизовані правила обміну інформацією з контрагентами. Це включає визначення форматів файлів, протоколів передачі даних і частоти синхронізації. Завдяки таким заходам можна знизити ризики втрати або пошкодження інформації під час її передачі між організаціями. Договори з партнерами повинні передбачати умови безпеки інформаційних потоків, що гарантує узгодженість внутрішніх стандартів підприємства з зовнішніми вимогами.

Не менш важливим аспектом є регулярний моніторинг і перевірка програмного забезпечення, яке використовується для автоматизації облікових процесів. Такий моніторинг дозволяє своєчасно виявляти і запобігати можливим шахрайським діям, а також забезпечує відповідність програмного забезпечення чинним вимогам бізнесу та законодавства. Регламентування оновлень та тестування програмного забезпечення сприяє підвищенню його ефективності, дозволяючи враховувати сучасні виклики та потреби підприємства.

Інтеграція правових, технічних і організаційних заходів у рамках кібербезпекових регламентів забезпечує комплексний захист інформаційних ресурсів. Такий підхід є надзвичайно важливим в умовах постійного зростання обсягів кіберзагроз. Впровадження цих регламентів дозволяє підприємствам не лише зберігати свої дані в безпеці, але й підвищувати загальну ефективність управління, що є критично важливим для довгострокової стабільності та конкурентоспроможності.

Перелік використаної літератури:

1. Мороз Ю.Ю., Цаль-Цалко Ю.С. 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. URL: <http://surl.li/flaezk>
2. Герасимович І. А. Організація облікової політики сучасного підприємства. Інвестиції: практика та досвід. 2018. № 7. С. 49–53. URL: <http://surl.li/ddrjut>
3. Кафка С. М. Етапи формування облікової політики. Актуальні проблеми розвитку регіональної економіки. 2017. № 1. Р. 156–164. URL: <https://doi.org/10.15330/apred.1.13.156-164>.
4. Лоханова Н. О. Облікова політика як інструмент управління економічною безпекою компанії. Інвестиції: практика та досвід. 2014. № 11. С. 12–16.

5. Закон України «Про бухгалтерський облік та фінансову звітність в Україні» від 16.07.1999 № 996-XIV. URL: <https://zakon.rada.gov.ua/laws/show/996-14#Text>

6. Наказ Міністерства фінансів України «Про затвердження Методичних рекомендацій щодо облікової політики підприємства та внесення змін до деяких наказів Міністерства фінансів України» від 27.06.2013 № 635. URL: <https://zakon.rada.gov.ua/rada/show/v0635201-13#Text>

Душкін С.С.

доцент

Харківський національний автомобільно-дорожній університет

ФОРМУВАННЯ ЕКОЛОГІЧНОЇ СВІДОМОСТІ ЗДОБУВАЧІВ У КОНТЕКСТІ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «СТРАТЕГІЯ СТАЛОГО РОЗВИТКУ ДЕРЖАВНОЇ КЛІМАТИЧНОЇ ПОЛІТИКИ»

Сталий розвиток – це загальна концепція, яка підкреслює важливість досягнення рівноваги між задоволенням поточних потреб людства та захистом інтересів майбутніх поколінь, включаючи їхню потребу в безпечному та здоровому навколишньому середовищі.

Змінні умови навколишнього середовища вимагають постійного вдосконалення систем управління екологією для забезпечення сталого розвитку. Розуміння цих взаємозв'язків і застосування системного підходу може підвищити ефективність та взаємодоповнюваність екологічних управлінських систем на національному, регіональному та міжнародному рівнях. Для цього потрібні висококваліфіковані фахівці в галузі охорони навколишнього середовища.

Концепція сталого розвитку людини, суспільства та навколишнього середовища передбачає перегляд орієнтирів у системі навчальних дисциплін екологічного спрямування. Традиційно екологічні дисципліни акцентують увагу на необхідності збереження довкілля для уникнення шкідливого впливу забруднення на людину, при цьому людина та суспільство розглядаються окремо від природи та довкілля. Вчені-екологи та педагоги підкреслюють необхідність подолання антропоцентричних стереотипів мислення у людей. Навчальна дисципліна відповідає цим потребам, навчаючи усвідомлювати себе як невід'ємну частину природи та бачити свій громадський обов'язок у збереженні та примноженні природи та довкілля.

Метою навчальної дисципліни є встановлення закономірностей розвитку відкритих стаціонарних систем, визначення взаємозв'язків енергетичної та інформаційної характеристик трансформаційних процесів та вивчення базових принципів, методів і інструментарію забезпечення стійкого розвитку суспільних систем з урахуванням кліматичної складової.

Основна мета навчальної дисципліни полягає у створенні умов для ефективного вирішення наявних навчально-виховних проблем у сфері виховання та формування екологічно свідомої особистості, яка живе в гармонії з природою, піклується про навколишнє середовище, створюючи належні умови для збереження та примноження біорізноманіття та існуючих екосистем, формуючи екологічно безпечне довкілля для сталого розвитку суспільства та особистості.

Відповідно до [1] стратегія формування та реалізації державної політики у сфері зміни клімату на період до 2035 року передбачає досягнення кліматичної нейтральності, зменшення викидів парникових газів та адаптацію до змін клімату. Основними завданнями є:

- зменшення викидів парникових газів: Впровадження енергоефективних технологій та розвиток відновлюваних джерел енергії;
- адаптація до змін клімату: Розробка та впровадження заходів для зменшення вразливості до кліматичних змін;
- підвищення обізнаності населення: Проведення освітніх програм та інформаційних кампаній для підвищення екологічної свідомості громадян;
- міжнародне співробітництво: Активна участь у міжнародних ініціативах та угодах, спрямованих на боротьбу зі змінами клімату.

Основні напрями реалізації Стратегії:

- енергетика: Перехід на відновлювані джерела енергії, зменшення використання викопних видів палива, впровадження енергоефективних технологій.