"поглинув" Індекс цифрової трансформації регіонів України і цю інформацію натепер неможливо аналізувати. А такого роду інформація була б дуже корисною для ТГ.

Утруднює аналіз процесу цифровізації ТГ й те, що в складі місцевих бюджетів не виокремлено в окрему статтю видатків на цифровізацію. Вони конкретизовані лише в розріз купівлі комп'ютерної техніки (офісна техніка, сервери, комп'ютери та обладнання, телевізійна, радіо- та телекомунікаційна апаратура, системи керування) та окремих послуг (програмне забезпечення, послуги з обслуговування комп'ютерних систем).

Через вищезазначене єдиним методом дослідження процесу цифровізації ТГ залишається несистемний івент-аналіз, що обмежує можливості системного моніторингу процесу на рівні ТГ, веде до втрати керованості ним, співставності з ЄС в контексті євроінтеграції. Тому органи виконавчої влади центрального та регіонального рівнів мають налагодити релевантну статистику цифровізації на рівні ТГ.

Література:

1. Індекс цифрової трансформації регіонів України. Підсумки 2023 року. Міністерство цифрової трансформації України. 2023. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/reports/Індекс-цифрової-трансформації-регіонів-України-2023.pdf

Кіріченко О.В.
кандидат економічних наук, доцент
Павелко В.П.
магістр, здобувач гр. УФЕБ-23М
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

СИСТЕМА УПРАВЛІННЯ РИЗИКАМИ ЗОВНІШНІХ ЗАГРОЗ ДЛЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Сучасне бізнес-середовище, яке характеризується динамічними змінами та частковою непрозорістю, представляє собою платформу, де господарська діяльність стикається як з можливостями, так і із загрозами. Це робить питання забезпечення економічної безпеки підприємства надзвичайно важливими. Економічна безпека підприємства є складним та багатогранним поняттям, яке визначає стан, коли суб'єкт господарювання максимально захищений від різноманітних загроз. Вищий рівень економічної безпеки свідчить про зниження залежності фінансово-господарської діяльності підприємства від негативних сценаріїв, які можуть виникати внаслідок певних загроз. Загрози можуть бути поділені на зовнішні (екзогенні) та внутрішні (ендогенні) залежно від їх походження. Оскільки зовнішні загрози, на відміну від внутрішніх, не можуть бути повністю ліквідовані через їх незалежність від управлінських рішень, їм слід приділяти особливу увагу. Для протидії зовнішнім загрозам економічній безпеці підприємства керівництву необхідно розробити комплекс спеціальних заходів, які допоможуть запобігти негативним наслідкам, що можуть виникнути в результаті реалізації цих загроз. Таким чином, питання розробки заходів для забезпечення зовнішньої економічної безпеки є особливо актуальними в умовах сучасності.

Система управління ризиками зовнішніх загроз для економічної безпеки підприємства є комплексним інструментом, який включає в себе кілька ключових елементів: ідентифікацію ризиків, оцінку ризиків, розробку стратегій управління ризиками, моніторинг та контроль.

Першим кроком у створенні системи управління ризиками зовнішніх загроз є ідентифікація потенційних ризиків. Цей процес включає аналіз макроекономічних показників, політичної ситуації, змін в законодавстві, міжнародних відносин та інших факторів, які можуть вплинути на діяльність підприємства. Для цього використовуються методи SWOT-аналізу, PEST-аналізу та інші інструменти стратегічного аналізу [2].

SWOT-аналіз дозволяє виявити сильні та слабкі сторони підприємства, а також можливості та загрози, які можуть вплинути на його діяльність. PEST-аналіз, в свою чергу, фокусується на політичних, економічних, соціальних та технологічних факторах, які можуть вплинути на підприємство. Додатково можуть використовуватися методи дельфійського опитування, метод мозкового штурму та інші інструменти для більш детального аналізу зовнішніх загроз.

Після ідентифікації зовнішніх загроз необхідно провести їх оцінку. Оцінка ризиків включає визначення ймовірності настання загрози та можливих наслідків для підприємства. Для цього використовуються методи кількісного та якісного аналізу, такі як метод експертних оцінок, метод сценарного аналізу та інші.

Метод експертних оцінок передбачає залучення фахівців для оцінки ймовірності та наслідків різних загроз. Метод сценарного аналізу дозволяє розробити різні сценарії розвитку подій та оцінити їх вплив на підприємство. Кількісний аналіз може включати використання математичних моделей та статистичних методів для більш точної оцінки ризиків.

Результатом оцінки ризиків є формування переліку пріоритетних загроз, які потребують негайного втручання. Цей перелік дозволяє підприємству зосередити свої ресурси на найбільш значущих загрозах та розробити ефективні стратегії управління ризиками.

На основі результатів оцінки ризиків розробляються стратегії управління ризиками. Стратегії можуть включати такі заходи, як диверсифікація діяльності, страхування ризиків, створення резервних фондів, впровадження інноваційних технологій та інші. Важливо, щоб стратегії були інтегровані в загальну стратегію розвитку підприємства та відповідали його місії та цілям [1].

Диверсифікація діяльності дозволяє підприємству зменшити залежність від одного ринку або продукту, що знижує ризики, пов'язані з економічними кризами та змінами в законодавстві. Страхування ризиків дозволяє перекласти частину фінансових ризиків на страхові компанії, що зменшує можливі втрати для підприємства. Створення резервних фондів дозволяє підприємству мати фінансові ресурси для покриття непередбачених витрат, пов'язаних з зовнішніми загрозами. Впровадження інноваційних технологій дозволяє підприємству підвищити свою конкурентоспроможність та адаптуватися до змін в зовнішньому середовищі.

Ефективна система управління ризиками зовнішніх загроз передбачає постійний моніторинг та контроль за реалізацією розроблених стратегій. Моніторинг включає регулярний аналіз зовнішнього середовища, оцінку ефективності впроваджених заходів та корегування стратегій у разі необхідності. Контроль забезпечує виконання встановлених норм та процедур, а також своєчасне реагування на зміни в зовнішньому середовищі.

Моніторинг може включати використання систем раннього попередження, які дозволяють своєчасно виявляти потенційні загрози та приймати відповідні заходи. Контроль може включати регулярні аудити та перевірки, які дозволяють оцінити ефективність системи управління ризиками та виявити можливі проблеми.

Система управління ризиками зовнішніх загроз для економічної безпеки підприємства є важливим інструментом для забезпечення його стійкості та конкурентоспроможності. Впровадження такої системи вимагає комплексного підходу, який включає ідентифікацію загроз, оцінку ризиків, розробку стратегій управління ризиками та постійний моніторинг та контроль. Ефективне управління ризиками дозволяє підприємству не лише мінімізувати негативні наслідки зовнішніх загроз, але й використовувати їх як можливості для розвитку.

Успішне впровадження системи управління ризиками зовнішніх загроз вимагає залучення кваліфікованих фахівців, використання сучасних інструментів аналізу та постійного вдосконалення стратегій управління ризиками. Підприємства, які здатні ефективно керувати зовнішніми загрозами, мають більше шансів на успішне функціонування та розвиток в умовах невизначеності та змін [3].

Література:

1. Вербицька Г.Л. Публічні механізми розвитку інноваційної діяльності як фактор забезпечення економічної безпеки України. Актуальні проблеми розвитку економіки регіону. Вип 20. Т.2. 2024. doi: https://doi.org/10.15330/apred.2.20.86-95
2. Загурський В.Ф. Державно-інституційне забезпечення інноваційної моделі економіки. Економіка, управління та адміністрування. 2023. № 2. С. 144-149.
3. Іванова В. М. Проектування системи публічного управління у сфері зовнішньоекономічної безпеки України. Дніпровський науковий часопис публічного управління, психології, права. Випуск 3, 2022. С. 36-41. DOI https://doi.org/10.51547/ppp.dp.ua/2022.3.6

Кіріченко О.В.
кандидат економічних наук, доцент
Струтинський О.О.
магістр, здобувач гр. УФЕБ-23М
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

ОРГАНІЗАЦІЯ ПРОЦЕСУ УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У сучасних умовах динамічного розвитку глобальної економіки та стрімкого технологічного прогресу економічна безпека підприємства набуває критичного значення. В умовах жорсткої конкуренції та нестабільності зовнішнього середовища підприємства стикаються з різноманітними ризиками та загрозами, які можуть негативно вплинути на їх фінансовий стан та загальну стійкість. Серед таких ризиків можна виділити фінансові кризи, зміни в законодавстві, технологічні зміни, а також внутрішні та зовнішні економічні чинники. У зв'язку з цим, організація ефективної системи управління економічною безпекою стає ключовим фактором успішного функціонування та розвитку підприємства. Економічна безпека включає в себе захист фінансових ресурсів, інформаційних систем, а також стратегічних планів і проектів підприємства. Впровадження комплексних підходів до управління економічною безпекою дозволяє мінімізувати ризики, забезпечити стабільне функціонування підприємства та підвищити його конкурентоспроможність на ринку [3].

У зв'язку з цим, організація ефективної системи управління економічною безпекою стає ключовим фактором успішного функціонування та розвитку підприємства. Економічна безпека включає в себе захист фінансових ресурсів, інформаційних систем, а також стратегічних планів і проектів підприємства. Впровадження комплексних підходів до управління економічною безпекою дозволяє мінімізувати ризики, забезпечити стабільне функціонування підприємства та підвищити його конкурентоспроможність на ринку.

Основними елементами системи управління економічною безпекою є аналіз ризиків, розробка та впровадження заходів по їх мінімізації, моніторинг та контроль за виконанням цих заходів. Аналіз ризиків передбачає виявлення та оцінку потенційних загроз, які можуть вплинути на діяльність підприємства. На основі цього аналізу розробляються стратегії та тактики, спрямовані на попередження та зменшення негативних наслідків цих загроз [1].

Розробка та впровадження заходів по мінімізації ризиків включає в себе створення внутрішніх нормативних документів, проведення навчань та тренінгів для персоналу, а також застосування сучасних технологій та інструментів захисту. Наприклад, використання великих даних (big data) та штучного інтелекту (AI) дозволяє проводити більш точний аналіз ризиків та прогнозувати потенційні загрози. Кібербезпека також стає важливим аспектом, оскільки зростаюча кількість кібератак може завдати значної шкоди інформаційним системам підприємства. Впровадження заходів кібербезпеки, таких як шифрування даних, використання антивірусного програмного забезпечення та регулярне оновлення систем, є невід'ємною частиною загальної стратегії управління ризиками.