СОЦІАЛЬНО-КОМПЕТЕНТНЕ УПРАВЛІННЯ КОРПОРАЦІЯМИ В УМОВАХ ПОВЕДІНКОВОЇ ЕКОНОМІКИ

Матеріали Міжнародної науково-практичної конференції

18 лютого 2021 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ
ФАКУЛЬТЕТ ЕКОНОМІКИ ТА УПРАВЛІННЯ
КАФЕДРА ПІДПРИЄМНИЦТВА І МАРКЕТИНГУ
КАФЕДРА ЕКОНОМІКИ І ПРИРОДОКОРИСТУВАННЯ
ГРОМАДСЬКА ОРГАНІЗАЦІЯ ІНСТИТУТ ЕКОНОМІЧНИХ ТА ЕКОЛОГО-ЕНЕРГЕТИЧНИХ ДОСЛІДЖЕНЬ
EUROPEAN INSTITUTE OFFURTHER EDUCATION
WO'JT OF GMINA GROMADSKA, POLAND
UNIVERSITY OF ECONOMY IN BYDGOSZCZ, POLAND

СОЦІАЛЬНО-КОМПЕТЕНТНЕ УПРАВЛІННЯ КОРПОРАЦІЯМИ В УМОВАХ ПОВЕДІНКОВОЇ ЕКОНОМІКИ

Матеріали Міжнародної науково-практичної конференції

18 лютого 2021 року

Луцьк 2021

УДК 334.78.005.35(082)

В 69

Рекомендовано до друку науковою радою Волинського національного університету імені Лесі Українки (протокол № 3 від 25.03.2021 р.)

Рецензенти:

Чорний Р. С. – доктор економічних наук, професор, директор Нововолинського навчально-наукового інституту менеджменту, професор кафедри фундаментальних та спеціальних дисциплін Західноукраїнського національного університету

Ляшенко О. М. – доктор економічних наук, професор, проректор з науково-педагогічної роботи та забезпечення якості вищої освіти Луцького національного технічного університету

Соціально-компетентне управління корпораціями в умовах поведінкової економіки: [матеріали міжнар. наук.-практ. конф. (18 лютого 2021 р.)] / відп. ред. О.М. Павлова, К. В. Павлов, Л. В. Шостак, А. М. Лялюк – Луцьк, 2021. – 565 с.

У збірнику подано тези доповідей на Міжнародній науково-практичній конференції. У них відображено теоретичні основи, перспективи забезпечення ефективності суб'єктів господарювання, перспективи розвитку корпорацій в умовах розвитку неоіндустріальної економіки.

Для науковців, економістів, фахівців і всіх, хто цікавиться питаннями розвитку економічної системи України.

УДК 334.78.005.35(082)

номінального якоря.

Список використаних джерел:

1. Береславська О. І. Інфляційне таргетування: еволюція розвитку та українська практика. Наукові записки Національного університету «Острозька академія». Серія «Економіка» : науковий журнал. Острог : Вид-во НаУОА, вересень 2018. № 10(38). С. 46–51.

2. Коць О. О. Інфляційне таргетування як стратегія ГКП: закордонний та вітчизняний досвід / О. О. Коць, П. Г. Ільчук, І. Л. Данилів // Економіка та суспільство. Електронне наукове Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua 59 фахове видання. – 2017. – №11. – С. 426

3 .Лейонхуфвуд А. Макроэкономическая теория в двадцатом столетии: основные вехи развития. *Вопросы экономики*. 2006;(11):26-45. https://doi.org/10.32609/0042-8736-2006-11-26-45

Лобода О. М., к.т.н., доцент
ХДАЕУ, м. Херсон, Україна

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦТВА

В сучасних умовах інформаційні ресурси мають істотне значення в розвитку науки, техніки, виробництва, сфери послуг та інших галузевих складових. Виникає проблема класифікації інформаційних ресурсів, обмеження доступу до деякої частини з них, термін економічної доцільності організації захисту інформації на підприємствах та в організаціях різноманітних сфер господарської діяльності. Інформаційна безпека з точки зору економічної безпеки являють собою стан захищеності діяльності організації та її інформаційного середовища від негативного впливу дестабілізуючих факторів, що забезпечує зберігання основних властивостей інформації та досягнення соціально-економічної мети створення організації.

Інформаційна загроза має місце тоді, коли величина та ймовірність можливого інформаційного збитку більше визначеного порогового значення, що потребує прийняття комплексу мір по його запобіганню, захисту об'єкту безпеки. Під загрозою безпеки інформації розуміються події або дії, які можуть призвести до спотворення, несанкціонованому використанню або навіть до руйнування інформаційних ресурсів управляючої системи, а також програмних і апаратних засобів [1, с.23]. Загроза збереження цілісності та конфіденційності інформаційних ресурсів обмеженого доступу практично реалізується через ризик утворення каналу несанкціонованого здобуття цінної інформації та документів. Функціонування каналу несанкціонованого доступу до інформації обов'язковим тягне за собою втрату інформації, зникнення носія інформації. Забезпечення інформаційної безпеки повинна починатися з виявлення суб'єктів відносин, пов'язаних з використанням інформаційних систем. Спектр їх інтересів може бути розподілений, на наступні категорії: доступність, цілісність та конфіденційність [2, с.103].

Тобто, в найбільш загальному вигляді інформаційна безпека може бути визначена як неможливість нанесення шкоди властивостям об'єкту безпеки, що обумовлюється інформацією та інформаційною інфраструктурою. К об'єктам інформаційної безпеки в організації відносять: інформаційні ресурси, які містять

відомості, що відносяться до комерційної таємниці та конфіденційну інформацію, яка представлена у вигляді інформаційних масивів та баз даних; засоби та системи інформатизації; засоби комп'ютерної та організаційної техніки; мережі та системи; загальне системне та прикладне програмне забезпечення; автоматизовані системи управління в організаціях; системи зв'язку та передачі даних; технічні засоби збору; реєстрації, передачі, обробки та відображення інформації [3, с.61]. До основних загроз безпеки відносять: розкриття конфіденційної інформації; несанкціоноване використання інформаційних ресурсів; помилкове використання ресурсів; несанкціонований обмін інформації; злом системи; компрометація.

До причин та умов, що створюють передумови для втрати інформації, може відноситись: недостатні знання співробітників організації правил захисту конфіденційної інформації та незрозумілість необхідності їх ретельного дотримання; використання неатестованих технічних засобів обробки конфіденційної інформації; слабкий контроль за дотриманням правил захисту інформації правовими організаційними та інженерно-технічними мірами та ін. Захист інформації - це комплекс мір, які направлені на забезпечення важливих аспектів інформаційної безпеки: цілісності, доступності та конфіденційності інформації й ресурсів, що використовуються для введення, зберігання, обробки та передачі даних. З позиції системного підходу до захисту інформації висуваються певні умови: забезпечення безпеки інформації не може бути одноразовим актом; це безперервний процес, який полягає в обґрунтуванні та реалізації найбільш раціональних методів, засобів та шляхів удосконалення та розвитку системи захисту, неперервному контролі її стану, виявлення її вузьких та слабких місць та протиправних дій; планування безпеки інформації виконується шляхом розробки кожною службою детальних планів захисту інформації у сфері її компетентності; захисту інформації потребують конкретних даних, які об'єктивно підлягають охороні, втрата яких може спричинити організації значну втрату; методи та засоби захисту повинні надійно перекривати можливі шляхи неправомірного доступу, ефективність захисту інформації означає, що затрати на її виконання не можуть бути більше можливих втрат від реалізації інформаційних загроз; чітко визначені повноваження та прав користувача на доступ до визначених видів інформації; надання користувачу мінімальних повноважень, які необхідні йому для виконання дорученої роботи; зведення до мінімуму числа загальних для декілька користувачів засобів захисту; облік випадків несанкціонованого доступу до конфіденційної інформації; забезпечення ступенів конфіденційної інформації; забезпечення контролю цілісності засобів захисту та негайне реагування на їх вихід із строю.

Отже, система захисту інформації повинна мати визначені види власного забезпечення: правове забезпечення, тобто нормативні документи, положення, інструкції; організаційне забезпечення, тобто реалізація захисту інформації, що виконується визначеними структурними одиницями, тобто служба безпеки, служба режиму, служба захисту інформації, технічними засобами та ін.; апаратне забезпечення; інформаційне забезпечення; програмне забезпечення математичне забезпечення; нормативно-методичне та ергономічне забезпечення. Таким чином, зміст складових частин елементів, методи та засоби захисту інформаційних ресурсів в рамках будь-якої системи захисту повинні постійно змінюватися з метою

запобігання їх розкриття зацікавленою особою.

Список використаних джерел:

1. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. Х.: ХНЕУ, 2018. 510 с.

2. Лобода О.М., Кириченко Н.В. Базові комунікаційні технології: навч. посіб. Херсон: Стар, 2018. 235 с.

3. Лобода О.М. Захист інформації в корпоративних мережах. *Публічне управління та адміністрування у процесах економічних реформ*: матеріали IV Всеукр. наук.-практ.конф., м. Херсон, 11 лист. 2020р. ХДАЕУ, 2020. С.61-63.

Матвієнко-Біляєва Г. Л., к.е.н., доц.
ХНЕУ ім. С. Кузнеця, м. Харків, Україна

АНТИКРИЗОВЕ УПРАВЛІННЯ ЯК СКЛАДОВА ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВ

В умовах ринкової економіки переважна більшість суб’єктів господарювання є відносно самостійними у прийнятті економічних рішень та самі несуть відповідальність за наслідки їх реалізації. В діяльності кожного підприємства періодично виникають ситуації, коли необхідно вживати заходи, спрямовані на запобігання виникненню кризових явищ, що є передумовою успішного фінансового оздоровлення підприємств, чи ліквідацію вже наявних ознак кризи.

Не стійка кон'юнктура ринкового середовища вимагає постійного діагностування та впровадження в менеджмент спеціальних антикризових заходів, як запоруки успішного функціонування підприємств. Тому особливої актуальності в умовах спаду економічного зростання набув процес розробки та використання ефективних методів і форм здійснення антикризового управління на підприємстві.

За останні роки виникли підприємства, що не розраховуються зі своїми партнерами, державою та працівниками, ці підприємства стають генераторами ланцюгової реакції неплатежів, що створює негативні тенденції в економіці країни, до таких підприємств необхідно застосовувати заходи, спрямовані на їхнє фінансово-господарське оздоровлення шляхом санації, реструктуризації, або добровільної ліквідації.

Не стійка кон'юнктура ринкового середовища вимагає постійного діагностування та впровадження в менеджмент спеціальних антикризових заходів, як запоруки успішного функціонування підприємств.

В сучасних умовах діяльності підприємств необхідним є створення механізму, за допомогою якого б здійснювався аналіз і попередження виникнення банкрутства. Саме таким механізмом є антикризове управління. Необхідність антикризового управління визначається цілями розвитку соціально-економічних систем і існуванням небезпеки виникнення кризи.

Останніми роками значно зросла кількість досліджень та публікацій стосовно антикризового управління. Перш за все, це пояснюється глибинною кризою, що охопила більшість підприємств різних галузей. Багато уваги було приділено питанням ефективності та дієвості антикризового управління, виникненню та попередженню кризових явищ на підприємстві. Питання антикризового управління в своїх працях досліджували багато вітчизняних та закордонних науковців,