наслідки по окремим фінансовим операціям, з якими ці ризики не пов'язані. Основними формами цього напрямку нейтралізації фінансових ризиків є: формування резервного фонду підприємства, цільових резервних фондів, системи страхових запасів матеріальних і фінансових ресурсів по окремих елементах оборотних активів підприємства[2].

Таким чином, розробка внутрішнього механізму нейтралізації фінансових ризиків пов’язана з вибором методів мінімізації їх негативних наслідків, які системно використовують в рамках самого підприємства.

За умов зростання рівня конкуренції кожне підприємство повинно своєчасно ідентифікувати і правильно оцінювати ступінь фінансових ризиків, що забезпечить можливість ефективного управління ними. Створення та впровадження механізму нейтралізації фінансових ризиків як складової системи економічної безпеки підприємства дозволить зменшити як ймовірність виникнення фінансових ризиків, так й їх негативний вплив на діяльність підприємства в цілому

Список літератури:

1. Крамаренко Г.О., Чорна О.Є. Фінансовий менеджмент: Підручник. – Київ: Центр навчальної літератури, 2006. – 207-210с.
2. Ковальова А.М., Лапуста М.Г., Скамай Л.Г. Фінанси фірми: Підручник. – М.:ИНФРА-М, 2000. – 67с.

Шолом А.І., к.е.н. Башинська І.О.

МІЖНАРОДНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ БЕЗПЕКИ (ПОЛІТИКА КОРОЛІВСТВА ШВЕЦІЇ)

Одеський національний політехнічний університет, Одеса

Створення сприятливих умов для розвитку бізнесу та реалізації права на підприємництво є невід'ємною складовою розвитку та економічної безпеки України, пріоритетною функцією уряду. Належний рівень бізнесу економічної безпеки є ключем до соціально-економічного розвитку, так як ринок, в якому конкуренція є основним компонентом, що загрожує. Прогалини у правовому полі держави, загальна фінансова нестабільність створює додаткові труднощі для ефективного управління. Інформаційна сфера являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, розповсюдження і використання інформації, а також системи регулювання виникаючих при цьому громадських відносин [1].

Важливість вивчення теоретичних засад та розробка прикладних рекомендацій щодо підвищення рівня забезпечення інформаційно-аналітичної безпеки підприємства в країнах, які переходять до ринкових відносин, зумовлена, в першу чергу, призупиненням темпів розвитку бізнесу в умовах виходу зі світової фінансової кризи. Відповідно необхідні проведення системно-структурного аналізу та імплементація позитивного світового досвіду забезпечення інформаційно-аналітичної складової економічної безпеки підприємства.

Метою даної роботи є виявлення особливостей політики Королівства Швеції щодо забезпечення інформаційно-аналітичної безпеки для перейняття позитивного досвіду українськими підприємствами.

Загрозами національної безпеки Королівства Швеції в інформаційній сфері є сукупність умов та чинників, які становлять небезпеку життєве важливим інтересам держави суспільства і особи у зв’язку з можливістю негативного інформаційного впливу на свідомість та поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру.

В механізмі забезпечення інформаційної безпеки мають бути враховані національні інтереси в інформаційному середовищі, внутрішні та зовнішні загрози цим інтересам і передбачена система засобів виявлення та нейтралізації загроз. Механізм має включати двосторонній зв'язок між суспільством, засобами масової інформації й державою, він допоможе своєчасно сповістити про зміни громадської думки та оцінювати ефективність ужитих заходів. Саме тому у Швеції діє програма «електронний уряд».

Електронний уряд фокусується на використанні нових інформаційних і комунікативних технологій урядом, які застосовуються до повного спектру управлінських функцій.

Прийняті рамкові документи – Програму 2020 (документ базується на Лісабонській стратегії) та Міністерську декларацію 2009 року, прийнятий в м. Малмьо (Швеція) на Міністерській конференції та встановлює цілі на 5 років, зокрема:

- посилення мобільності всередині єдиного ринку;
- посилення ефективності та результативності Уряду при скороченні адміністративних бар'єрів через використання інформаційних технологій;
- надання повноважень громадянам та бізнесу.

Проте залишається значна різниця між результатами послуг для бізнесу і послуг для громадян.

У Швеції та ще 5 Провідних країн (Австрія, Мальта, Португалія, Сполучене Королівство), в яких повністю доступні онлайн 20 основних послуг [2].

Одним з головних засобів забезпечення інформаційної безпеки є правове регулювання засобів масової інформації.

Конституція Швеції гарантує всім громадянам «у їхніх відносинах із державною службою вільне одержання будь-якої інформації або можливість ознайомитися з іншими думками», передбачено захист прав громадян на одержання необхідної інформації.

Дослідники М. Прайс та П. Круг виокремлюють чотири основні аспекти правового середовища, в якому діють засоби масової інформації та завдяки якому законодавство або сприяє, або перешкоджає їх незалежності й ефективності:

- збір інформації;
- регулювання змісту;
- нейтральне стосовно змісту регулювання, яке водночас здатне впливати на зміст побічно;
- захист журналістів у процесі їхньої професійної діяльності, у тому числі захист від фізичного нападу [3].

Відповідно до оцінок шведських військових аналітиків – інформаційна зброя стане основним засобом ведення негласної війни, з огляду на залежність розвинених держав, яка підсилюється від систем зв'язку та інформації. Тому, для адекватного захисту країни в ході інформаційної війни, необхідно, насамперед, створити ефективну систему державного управління і контролю.

Список літератури:

1. Башинська І.О. Розділ 3.2. Уточнення визначення дефініції та економічного змісту категорії «економічна безпека підприємства» (С. 14-20) у кол. монографії Економічна безпека в умовах глобалізації світової економіки : [колективна монографія у 2т.]. – Дніпропетровськ: «ФОП Дробязко С.І.», 2014. – Т. 2. – 349 с.
2. Почепцов Г.Г., Чукут С.А. Інформаційна політика: Навч. посіб. 2-ге вид., стер. – К.: Знання, 2008. – 663 с.
3. Соціально-правові основи інформаційної безпеки: навч. посіб. / В.М. Петрик, А.М. Кузьменко, В.В. Остроухов, О.А. Штоквич, В.І. Полевий; Укр. акад. наук, Держ. ун-т інформ.-комунікац. технологій. – К.: Росава, 2007. – 496 с.