DOI: https://doi.org/10.32782/2524-0072/2022-44-30

УДК 338.91

ПРОГРЕСИВНІСТЬ РОЗВИТКУ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

PROGRESSIVE DEVELOPMENT OF THE CORPORATE INFORMATION PROTECTION SYSTEM

Чубаєвський В.І.
кандидат політичних наук, доцент,
Державний торговельно-економічний університет
ORCID: https://orcid.org/0000-0001-8078-2652

Chubaievskyi Vitaliy
State University of Trade and and Economics

У статті визначено, що обов'язковою умовою забезпечення ефективної та рентабельної діяльності корпоративних структур є підвищення ролі системи захисту корпоративної інформації в управлінні їх розвитком. Науково обґрунтована об'єктивна необхідність розробки такої стратегії інформаційної безпеки, яка забезпечувала би гнучкість корпоративних структур в умовах економічної, соціальної та політичної динаміки і сприяла би можливості для прийняття ефективних рішень на основі адаптивних підходів в управлінні корпоративними структурами. Доведено, що ефект гнучких корпоративних систем, слід визначити як «стратегічний» ефект гнучкого реагування корпоративної політики інформаційної безпеки на зміну потреб корпорацій. Необхідність досягнення такого стратегічного ефекту висуває вимоги повноти обліку витрат на створення та функціонування політики інформаційної безпеки корпоративної структури, яка була б здатна такий ефект спричинити. Визначені найважливіші умови досягнення стратегічного ефекту системи захисту корпоративної інформації щодо величини витрат, пов'язаних із створенням, реалізацією та кінцевого результату впровадження цієї системи. Науково обґрунтовано, що під прогресивністю розвитку системи захисту корпоративної інформації слід розуміти її пристосованість до ефективного, своєчасного та якісного досягнення цілей і завдань функціонування корпорацій, що володіє певним і постійно повторюваним ступенем різноманітності напрямів корпоративної політики інформаційної безпеки.

Ключові слова: корпоративні структури, корпоративна інформація, система захисту корпоративної інформації, корпоративна політика інформаційної безпеки, прогресивність розвитку системи захисту корпоративної інформації.

The article determines that a prerequisite for ensuring the effective and profitable operation of corporate structures is to increase the role of the corporate information security system in managing their development. The objective necessity of developing such an information security strategy, which would ensure the flexibility of corporate structures in the conditions of economic, social and political dynamics and would facilitate the possibility of making effective decisions based on adaptive approaches in the management of corporate structures, is scientifically substantiated. It is proved that the effect of flexible corporate systems should be defined as a "strategic" effect of flexible response of corporate information security policy to the changing needs of corporations. The need to achieve such a strategic effect requires a complete accounting of the costs of creating and operating the information security policy of the corporate structure, which would be able to cause such an effect. The most important conditions for achieving the strategic effect of the corporate information security system in terms of the amount of costs associated with the creation, implementation and the final result of the implementation of this system are determined. Generalization and systematization of the composition of costs associated with the creation and implementation of the corporate information protection system allowed to outline the main prerequisites for obtaining the strategic effect of flexible response to changes in the goals of the corporate structure. It is proved that the ability of the corporate information security protection system to respond flexibly to changes in the needs of the corporation is determined by the ratio of the rate of change in the degree of corporate information security policy and the rate of change in costs that ensure its effective functioning over a certain period. It is scientifically substantiated that the progressiveness of the development of the corporate information security system should be understood as its adaptability to the effective, timely and high-quality achievement of the goals and objectives of the functioning of corporations, which has a certain and constantly recurring degree of diversity of corporate information security policy.

Keywords: corporate structures, corporate information, corporate information protection system, corporate information security policy, progressive development of corporate information protection system.

Постановка проблеми. Корпоративні структури – це динамічні системи зі складною внутрішньою структурою та різнобічними зв'язками між елементами, які цілеспрямовано забезпечують своє функціонування та взаємодію із зовнішнім середовищем.

В основі організації корпоративних структур лежить системний підхід. Методологія системного підходу полягає в виявленні тих аспектів предметів чи подій, які випливають із загальних властивостей системи. Дослідження ступеня розвитку систем та механізмів їх функціонування в умовах економічного середовища, що змінюється, становить основу дослідження корпоративних структур, їх властивостей, структури, організованості та функціонування з урахуванням взаємодії із зовнішнім економічним середовищем. Різноманітність властивостей, елементів корпоративних структур, їх призначення та зв'язки дозволяють зробити висновок, що вони відносяться до класу складних динамічних систем.

Отже, в даний час важливим для корпоративних структур є розробка такої стратегії інформаційної безпеки, яка забезпечувала би гнучкість корпоративних структур в умовах економічної, соціальної та політичної динаміки і сприяла би можливості для прийняття ефективних рішень на основі адаптивних підходів в управлінні корпоративними структурами.

Звідси обов'язковою умовою забезпечення ефективної та рентабельної діяльності корпоративних структур є підвищення ролі корпоративної політики інформаційної безпеки в управлінні їх розвитком.

Аналіз останніх досліджень і публікацій. Питання прогресивності розвитку систем захисту корпоративної інформації досліджували такі вітчизняні та зарубіжні вчені як: З. Валіулліна [1], В. Домарєв [2], В. Гордієнко [2], О. Жабинець [3], С. Парк [4], Т. Руіджхавер [4], К. С. Хонг [5] та інші.

Однак, сучасний розвиток корпоративної політики інформаційної безпеки, в основі якої переважають соціально-економічні стимули, призвів до необхідності розширення досліджень кола питань щодо визначення відповідного рівня прогресивності розвитку систем захисту інформації, який дозволяє гнучко реагувати на зміну потреб корпорацій.

Метою статті є обґрунтування необхідності та доцільності визначення прогресивності розвитку системи захисту корпоративної інформації.

Виклад основного матеріалу дослідження. Корпоративна політика інформаційної безпеки, в основі якого лежать переважно соціально-економічні стимули розвитку корпорацій, сприяє істотному розширенню їх самостійності. Вона проявляється як у виборі цілей розвитку, так і у виборі засобів досягнення цих цілей.

Можливість варіювання цілей та маневрування ресурсами, що виникає під впливом корпоративної політики інформаційної безпеки, позначається на прогресивності динамічного розвитку корпорацій.

Ефект гнучких корпоративних систем, що включає всі елементи, слід визначити як «стратегічний» ефект гнучкого реагування корпоративної політики інформаційної безпеки на зміну потреб корпорацій.

Необхідність досягнення такого стратегічного ефекту висуває вимоги повноти обліку витрат на створення та функціонування політики інформаційної безпеки корпоративної структури, яка була б здатна такий ефект спричинити. Це становище випливає із відомого закону необхідної різноманітності. Тут слід враховувати принаймні дві найважливіші обставини.

По-перше, щодо величини витрат, пов'язаних із створенням і реалізацією корпоративної політики інформаційної безпеки, необхідно вибрати як об'єкт економічного аналізу таку сукупність технічних, технологічних, трудових, інформаційних, просторових і структурних ресурсів, яка була б здатна функціонувати автономно.

По-друге, гнучка політика інформаційної безпеки корпоративних структур, що створюється, повинна бути настільки значущою з точки зору кінцевого результату діяльності корпорацій, частиною якої вона є, щоб забезпечити можливість отримання всіх або принаймні найбільш значущих складових стратегічного ефекту.

Такий об'єкт, що відповідає вимогам автономності та значущості, назвемо первинним модулем гнучкої корпоративної політики інформаційної безпеки, витрати на створення та функціонування якого можуть створити передумови для отримання стратегічного ефекту гнучкого реагування на зміну цілей корпоративної структури. При визначенні складу корпоративної політики інформаційної безпеки слід враховувати і ефект цілісності (принцип емерджентності), що виражає таку важливу властивість системи: чим більша система і чим більша різниця в розмірах між

частиною та цілим, тим частіше ймовірність того, що властивості цілого можуть сильно відрізнятиметься від властивостей частин [4].

Це означає, що чим менший об'єкт прийнятий як модуль гнучкої корпоративної політики інформаційної безпеки, тим менш ймовірне досягнення за допомогою цього об'єкта в повному обсязі стратегічного ефекту гнучкого реагування на зміну потреб суспільства. Нехтування цим принципом призводить до того, що на підприємствах створюються дрібні гнучкі об'єкти для забезпечення їхньої інформаційної безпеки, лінії та інші підрозділи, які не можуть забезпечити виникнення передумов для отримання ефекту, достатнього для окупності капітальних вкладень. З чого робиться висновок (іноді необгрунтований) про потенційну неможливість створення високоефективних гнучких інструментів реалізації корпоративної політики інформаційної безпеки або необхідність розробки спеціальних методик визначення їхньої економічної ефективності, покликаних штучно підвищити ефект у сфері функціонування корпорацій.

Вибір модуля корпоративної політики інформаційної безпеки пов'язаний також із відомою закономірністю інтегративності системи, що передбачає наявність факторів, що забезпечують її збереження, тобто системоутворюючих, системозберігаючих факторів. Що стосується гнучкої корпоративної політики інформаційної безпеки подібним системоутворюючим чинником є значимість елементів системи з погляду їхнього впливу ступінь гнучкості всієї системи.

У кожній корпоративній системі можуть бути знайдені провідні елементи, від яких залежить визначальною мірою здатність системи досягати заданих цілей. Інакше якщо елемент системи має надмірну жорсткість, що не дозволяє всій системі ефективно, своєчасно та якісно переходити від виготовлення однієї продукції до іншої, він має стати насамперед основою створення модуля гнучкої корпоративної політики інформаційної безпеки. Якщо таких елементів системи кілька, то як основа модуля гнучкої корпоративної політики інформаційної безпеки повинна бути прийнята сукупність цих елементів системи. Ігнорування цього положення не дозволить досягти очікуваного ефекту, а вкладені кошти виявляться омертвленими.

Таким чином, для кожного модуля гнучкої корпоративної політики інформаційної безпеки або їх сукупності повинен бути визначений оптимальний з точки зору співвідношення витрат та потенційного стратегічного ефекту прогресивність корпоративної системи, що забезпечує високий рівень ефективності задоволення потреб корпорації.

Зміна потреб суспільства відбивається на прогресивності корпоративної політики інформаційної безпеки. У міру збільшення темпів зміни потреб, що виражаються у збільшенні темпів оновлення продукції, прогресивність корпоративної політики інформаційної безпеки має посилюватись. Інакше корпорація змушена перебуватиме у стані постійного переозброєння чи реконструкції. Посилення прогресивності неминуче пов'язане зі зростанням ступеня виробничої різноманітності продукції, що випускається корпорацією [5].

Отже, кількісною характеристикою зміни потреб суспільства за той чи інший період може стати індекс зміни за цей період ступеня розмаїття заходів корпоративної політики інформаційної безпеки, $I_{пр}(t_h,t_k)$ – де, t_h,t_k – де, – відповідно початок і кінець аналізованого періоду. Економічною характеристикою задоволення потреб, що змінюються, за той же період може бути прийнятий індекс зміни витрат, пов'язаних з функціонуванням корпоративної політики інформаційної безпеки $I_{п}(t_h,t_k)$. Тоді кількісною характеристикою гнучкості корпоративної політики інформаційної безпеки може бути показник:

$$G(t_h,t_k) = I_{пр}(t_h,t_k) \qquad (1)$$

У міру збільшення ступеня гнучкості системи за аналізований період все більше відрізнятиметься від одиниці (у більшу сторону). Це означає, що чим вище темпи зміни ступеня різноманітності заходів корпоративної політики інформаційної безпеки порівняно з темпами зміни витрат, пов'язаних зі створенням та функціонуванням системи, тим інформаційна безпека має більший рівень гнучкості.

Якщо $G(t_h,t_k) < 1$, то створена система інформаційної безпеки корпорації повинна бути віднесена до категорії жорстких систем, при $G(t_h,t_k) = 1$ система адаптивна. Якщо $G(t_h,t_k) > 1$ система гнучка.

Дуже важливим при розрахунку показника $G(t_h,t_k)$ є визначення вимірювачів ступеня різноманіття напрямів корпоративної політики інформаційної безпеки, пов'язаних із створенням та функціонуванням корпоративних структур.

Як вимірник ступеня різноманіття напрямів корпоративної політики інформаційної безпеки у найпростішому випадку, як було показано вище, може бути використаний

коефіцієнт асоціації. Тоді значення $I_{np}(t_h,t_k)$ визначаються за формулою:

$$I_{np}(t_h,t_k) = [1 - S(t_h,t_k)] / [1 - S(t_h)], \quad (2)$$

де $S(t_h,t_k)$, $S(t_h)$ – коефіцієнти асоціації відповідно за весь період та на початок періоду.

Як вимірник витрат, пов'язаних зі створенням та реалізацією, можуть бути прийняті витрати за період (t_h,t_k). Однак при цьому слід особливо обумовити їхній склад. Це зумовлено важливими положеннями визначення потенційного стратегічного ефекту гнучкого реагування зміну потреб суспільства, викладеними вище.

Оскільки потенційний стратегічний ефект гнучкого реагування може бути забезпечений в результаті взаємодії всіх складових корпоративної політики інформаційної безпеки, так забезпечити передумови досягнення зазначеного ефекту можуть капітальні вкладення і поточні витрати, пов'язані зі створенням і функціонуванням цих складових.

Сукупність технічних, технологічних, кадрових, інформаційних та організаційно-економічних ресурсів дозволяє визначити узагальнений склад витрат, здатних спричинити виникнення потенційного стратегічного ефекту гнучкого реагування на зміну потреб корпорацій (табл. 1).

Дані, наведені у таблиці 1, можуть бути деталізовані з необхідною для тих чи інших цілей аналізу ступенем конкретизації. Для розрахунку кожної із складових одноразових чи поточних витрат розробляються відповідні моделі.

Результати цих розрахунків зводяться за допомогою наступного виразу:

$$Z(t_h,t_k) = \sum_{t=t_h}^{t=t_k} [(\sum_{i=1}^{i=h} C_{it} + \sum_{i=1}^{i=5} K_{it})(1 + E_h^Z)^{t_k - t}], \quad (3)$$

де C_{it} – поточні витрати на підтримку в актуальному стані i-ої умови функціонування корпоративної політики інформаційної безпеки у році t, $t \in (t_h,t_k)$;

K_{it} – одноразові витрати на формування i-ої умови функціонування корпоративної політики інформаційної безпеки на рік t, $t \in (t_h,t_k)$;

E_h^Z – коефіцієнт дисконтування різночасних витрат;

$Z(t_h,t_k)$ – витрати на створення та підтримання в актуальному стані умов функціонування корпоративної політики інформаційної безпеки у період (t_h,t_k).

Тоді

$$I_n(t_h,t_k) = Z(t_h,t_k) / Z(t_h), \quad (4)$$

де $Z(t_h)$ – витрати на створення та підтримання в актуальному стані умов функціонування корпоративної політики у першому році аналізованого періоду.

Підставивши значення $I_{np}(t_h,t_k)$ и у формулу (3), отримаємо кількісну характеристику

Таблиця 1

Склад витрат, що створюють передумови для ефективного функціонування корпоративної політики інформаційної безпеки

Напрями витрат	
Одночасні	**Поточні**
Формування технічних ресурсів корпоративної політики інформаційної безпеки – $К_1$	Підтримка технічних ресурсів корпоративної політики інформаційної безпеки в актуальному стані – $С_1$
Формування технологічних ресурсів корпоративної політики інформаційної безпеки – $К_2$	Підтримка технологічних ресурсів корпоративної політики інформаційної безпеки в актуальному стані – $С_2$
Формування кадрового потенціалу корпоративної політики інформаційної безпеки – $К_3$	Підтримка в актуальному стані кадрового потенціалу корпоративної політики інформаційної безпеки – $С_3$
Формування інформаційних ресурсів корпоративної політики інформаційної безпеки – $К_4$	Підтримка в актуальному стані інформаційних ресурсів корпоративної політики інформаційної безпеки – $С_4$
Формування організаційно-економічних ресурсів корпоративної політики інформаційної безпеки – $К_5$	Підтримка в актуальному стані організаційно-економічних ресурсів корпоративної політики інформаційної безпеки – $С_5$

гнучкості корпоративної політики інформаційної безпеки:

$$G(t_h,t_k)=\frac{[1-S(t_h,t_k)](\sum_{i=1}^{5}C_{it_h}+\sum_{i=1}^{5}K_{it_h})(1+E_h^z)^{t_k-1}}{[1-S(t_h)]\sum_{t=t_h}^{t_k}[(\sum_{i=1}^{5}C_{it}+\sum_{i=1}^{5}K_{it})(1+E_h^z)^{t_k-t}]}. \quad (5)$$

Таким чином, здатність корпоративної політики інформаційної безпеки до гнучкого реагування змін потреб суспільства визначається співвідношенням темпів зміни ступеня напрямів корпоративної політики інформаційної безпеки та темпів зміни витрат, що забезпечують її ефективне функціонування протягом певного періоду.

Інакше висловлюючись, здатність корпоративної політики інформаційної безпеки змінювати свою прогресивність без істотного збільшення сукупних витрат, які забезпечують її ефективне функціонування, має кваліфікуватися як гнучкість цієї системи.

Отже, під ефективністю системи захисту корпоративної інформації слід розуміти досягнення заданих системі цілей з мінімальними витратами та одночасним покращенням (в ідеальному випадку) або (принаймні) не заподіянням шкоди соціальній та екологічній системам.

В умовах високих темпів науково-технічного прогресу корпоративна політика інформаційної безпеки може успішно виконувати своє головне призначення, якщо вона спочатку має можливість протягом тривалого часу ефективно, своєчасно і якісно задовольняти потреби корпорації, що змінюються. Однак, ступінь різноманітності потреб, що задовольняються має бути визначена в певних межах. Тоді як основний чинник прогресивності корпоративна політика інформаційної безпеки слід розглядати сталість і повторюваність ступеня розмаїття її напрямів та інструментів.

Таким чином, під прогресивністю розвитку системи захисту корпоративної інформації слід розуміти її пристосованість до ефективного, своєчасного та якісного досягнення цілей і завдань функціонування корпорацій, що володіє певним і постійно повторюваним ступенем різноманітності напрямів корпоративної політики інформаційної безпеки.

Вихідним моментом процесу формування прогресивності системи захисту корпоративної інформації є визначення завдань економічного та соціального розвитку суспільства на найближчу перспективу. Необхідність вирішення цих завдань, їх характер і значущість визначають специфіку потреб суспільства, яка, своєю чергою, формулює вимоги до результативності діяльності корпорації, покликаної задовольняти ці потреби суспільства.

У різноманітті споживчих та виробничих властивостей діяльності та продукції корпоративних структур, обсягів потреби в ній та можливих обсягів, засобів та методів її виробництва об'єктивно проявляється процес поділу праці, який визначає галузеву, виробничу та організаційно-управлінську структуру діяльності корпорацій. Розширення потреб і розширення напрямів діяльності корпоративних структур створюють передумови для галузевої їх діяльності, а різноманіття технологій, обумовлене науково-технічним прогресом, є основою розвитку різних видів і напрямів спеціалізації діяльності корпорацій.

Висновки. Особливості прогресивності корпоративної політики інформаційної безпеки формують зворотні зв'язки з суспільними потребами та завданнями соціально-економічного розвитку країни. Ці зв'язки стимулюють чи, навпаки, стримують розвиток тих чи інших потреб. Надмірно мала прогресивність системи захисту корпоративної інформації має консервативність по відношенню до процесу оновлення діяльності корпорацій. У той самий час прогресивність корпоративної політики інформаційної безпеки стимулює прискорене розвиток потреб суспільства, створює сприятливі передумови підвищення ефективності задоволення нових потреб економіки та населення.

Таким чином, у процесі дослідження виникає проблема пошуку кращої прогресивності корпоративної політики інформаційної безпеки, тобто пошуку параметрів сфери ефективного функціонування системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Валіулліна З. В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів. *Вісник Дніпропетровського університету. Серія : Менеджмент інновацій*. 2016. Випуск 6. С. 34–41.

2. Домарєв В. В., Гордієнко О. В. Обґрунтування основних функцій системи управління інформаційною безпекою. *Вісник Державного університету інформаційно-комунікаційних технологій*. 2012. Т. 10, № 2. С. 102–104.

3. Жабинець О. Й. Політика інформаційної безпеки страхових компаній: українські реалії та досвід США. *Проблеми економіки*. 2014. № 4. С. 22–27.

4. Park, S., and Ruighaver, T. "Strategic Approach to Information Security in Organizations," *ICISS. International Conference on Information Science and Security*, 2008: IEEE, pp. 26–31.

5. Hong, K.-S., Chi, Y.-P., Chao, L., and Tang, J.-H. "An Integrated System Theory of Information Security Management," *Information Management & Computer Security.* 2003. 11:5. P. 243–248.

6. Kim, S. H., Wang, Q.-H., and Ullrich, J. B. "A Comparative Study of Cyberattacks," *Communications of the ACM.* 2012. 55:3. P. 66.

7. Soomro, Z. A., Shah, M. H. and Ahmed, J. “Information security management needs more holistic approach: a literature review”, *International Journal of Information Management,* 2016. Vol. 36 No. 2, pp. 215–225. DOI: https://doi.org/10.1016/j.ijinfomgt.2015.11.009.

REFERENCES:

1. Valiullina Z. V. (2016) Informatsiina bezpeka korporatyvnoi ekonomiky v umovakh hlobalizatsiinykh protsesiv. [Information security of the corporate economy in the context of globalization processes]. *Visnyk Dnipropetrovskoho universytetu. Seriia: Menedzhment innovatsii*, vol. 6, pp. 34–41. (in Ukrainian)

2. Domariev V. V., Hordiienko O. V. (2012) Obgruntuvannia osnovnykh funktsii systemy upravlinnia informatsiinoiu bezpekoiu. [Substantiation of the main functions of the information security management system]. *Visnyk Derzhavnoho universytetu informatsiino-komunikatsiinykh tekhnolohii*, vol. 10(2), pp. 102–104. (in Ukrainian)

3. Zhabynets O. Y. (2014) Polityka informatsiinoi bezpeky strakhovykh kompanii: ukrainski realii ta dosvid SShA. [Information security policy of insurance companies: Ukrainian realities and USA experience]. *Problemy ekonomiky*, vol. 4, pp. 22–27. (in Ukrainian)

4. Park S., Ruighaver T. (2008). "Strategic Approach to Information Security in Organizations," ICISS. International Conference on Information Science and Security, IEEE, 26–31.

5. Hong, K.-S., Chi, Y.-P., Chao, L., & Tang, J.-H. (2003). "An Integrated System Theory of Information Security Management," Information Management & Computer Security, (11:5), 243–248.

6. Kim, S. H., Wang, Q.-H., & Ullrich, J. B. (2012). "A Comparative Study of Cyberattacks". Communications of the ACM, (55:3), 66.

7. Soomro, Z. A., Shah, M. H. & Ahmed, J. (2016). “Information security management needs more holistic approach: a literature review”, *International Journal of Information Management,* 36, 2, 215–225. DOI: https://doi.org/10.1016/j.ijinfomgt.2015.11.009.