ЕКОНОМІКА ТА УПРАВЛІННЯ ПІДПРИЄМСТВАМИ

УДК 681.3
DOI: https://doi.org/10.32782/2224-6282/177-10

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

Богма О. С.
доктор економічних наук, доцент,
Київський національний торговельно-економічний університет
ORCID: https://orcid.org/0000-0002-5637-6010

Сілакова Г. В.
кандидат економічних наук, доцент,
Київський національний торговельно-економічний університет
ORCID: https://orcid.org/0000-0002-8083-5600

Chubaievskyi Vitalii, Bogma Olena, Silakova Hanna
Kyiv National University of Trade and Economics

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ ВІТЧИЗНЯНИХ ПІДПРИЄМСТВ

У статті обґрунтовано доцільність організації ефективних систем захисту інформації на вітчизняних підприємствах. Розглянуто сутність та мету функціонування системи захисту корпоративної інформації на підприємстві. Виокремлено основні складові системи захисту корпоративної інформації підприємства (функціональна, економічна та організаційна). З урахуванням виділеної структури системи захисту інформації запропоновано інтегральну методику оцінювання рівня ефективності системи захисту корпоративної інформації підприємства, яка передбачає розрахунок інтегральних показників за кожною виділеною складовою системи захисту корпоративної інформації підприємства й загального інтегрального показника. Розроблено шкалу інтерпретації рівня ефективності системи захисту корпоративної інформації підприємства за пропонованою методикою.

Ключові слова: *корпоративна інформація, система захисту інформації, інформаційна безпека, загроза, методика оцінки.*

METHODS OF EVALUATION OF EFFICIENCY OF CORPORATE INFORMATION PROTECTION SYSTEMS OF DOMESTIC ENTERPRISES

The article is devoted to the substantiation of the integrated methodology for assessing the effectiveness of corporate information protection systems of domestic enterprises, taking into account the selected components of the system. The relevance of the development of this methodology is due to the fact that due to the growing number of information crimes, the organization of effective systems for the protection of corporate information in domestic enterprises is a prerequisite for the survival of the enterprise. The issues of scientific and theoretical substantiation of the method of integrated evaluation of the effectiveness of corporate information protection systems of the enterprise are based on general scientific and special methods of cognition. Thus, methods of analysis and synthesis, induction and deduction, generalization are used to identify the main components of the system of protection of corporate information. A systematic approach was used to substantiate the author's methodology for evaluating the effectiveness of corporate information protection systems of the enterprise. The method of theoretical generalization and formulation of conclusions was used to formulate conclusions. Thus, the article substantiates the feasibility of organizing effective information protection systems at domestic enterprises. The essence and purpose of functioning of the system of protection of corporate information at the enterprise are considered. The main components of the corporate information protection system of the enterprise (functional, economic and organizational) are highlighted. Taking into account the allocated structure of the information protection system, an integrated method for assessing the level of efficiency of the corporate information protection system is proposed, which provides for the calculation of integrated indicators for each selected component of the corporate information protection system and the overall integrated indicator. The scale of interpretation of the level of efficiency of the corporate information protection system of the enterprise according to the proposed method is developed. The practical value of the developed methodology is that it is based on one of the basic principles of the system approach, which assumes that each component of the information security system, performing its function, ensures the achievement of the goal, which is, its information security.

Keywords: *corporate information, information protection system, information security, threat, assessment methods.*

JEL Classification: *C13, C80, C89*

Постановка проблеми. У мінливих та важко прогнозованих умовах сучасної ринкової економіки для підприємств будь-якої галузі існує гостра потреба забезпечення надійного захисту та збереження інформації (перш за все конфіденційної та секретної), що являє собою пріоритетне питання забезпечення інформаційної безпеки підприємства, якість вирішення якого справляє безпосередній вплив на інші функціональні складові економічної безпеки. Важливість захисту інформації підтверджується тим фактом, що за останні п'ять років в Україні кількість інформаційних злочинів зросла щонайменше у 2,5 рази [2]. Відтак, організація ефективних систем захисту корпоративної інформації на вітчизняних підприємствах сьогодні виступає об'єктивною необхідністю, яка забезпечує не лише необхідний і достатній рівень конкурентоспроможності й успіх в конкурентній боротьбі, але й саме виживання підприємства.

У зв'язку з цим розробка науково обґрунтованих методик оцінки ефективності систем захисту корпоративної інформації на підприємствах набуває особливої актуальності як у теоретичному, так і в практичному плані, адже дозволяє виявити слабкі місця, резерви та напрями оптимізації функціонування системи захисту інформації відповідного підприємства.

Аналіз останніх досліджень і публікацій. Проблемам створення, організації функціонування, оцінки ефективності, вдосконалення та розвитку систем захисту корпоративної інформації на підприємствах присвячені наукові праці таких зарубіжних і вітчизняних вчених, як В. В. Андріанов, О. І. Гарасимчук, В. Б. Голованов, С. М. Ілляшенко, Ю. М. Костів, В. Н. Максименко, Т. В Полозова, Ю. Я. Самохвалов, С. В Толюпа., О. В. Харкянен, Л. Дж. Хоффман, Н. В. Цьопа, Е. В. Ясюк та ін.

Аналіз наукових праць з проблеми розроблення підходів, методів та способів оцінки ефективності захисту інформації на підприємствах свідчить про недостатню розробленість теорії й методології проведення оцінки ефективності систем захисту корпоративної інформації вітчизняних підприємств. Зокрема, більш глибокого опрацювання потребують проблеми розробки науково-обґрунтованих універсальних методик оцінювання ефективності систем захисту корпоративної інформації вітчизняних підприємств в сучасних умовах господарювання.

Мета статті полягає в розробленні методики інтегрального оцінювання ефективності системи захисту корпоративної інформації підприємства з урахуванням виокремлених складових вказаної системи.

Виклад основного матеріалу. Забезпечення дієвого захисту інформації на підприємстві, який спрямований на попередження неправомірного й несанкціонованого доступу до інформації та її використання, витоку інформації, впливу програм-вірусів, неправомірної зміни даних та ін., потребує запровадження у практиці функціонування підприємств систем захисту корпоративної інформації

Система захисту корпоративної інформації являє собою складний комплекс програмних, технічних, криптографічних організаційних та інших засобів, методів та заходів, призначених для захисту інформації [3, с. 254]. Метою функціонування системи захисту корпоративної інформації є попередження виникнення та мінімізація негативного впливу загроз інформації внутрішнього й зовнішнього походження й, відповідно, забезпечення необхідного і достатнього рівня інформаційної безпеки підприємства. А її ефективність характеризується рівнем захищеності інформації підприємства від несанкціонованих й неправомірних дій у розрізі різноманітних критеріїв.

Відзначимо, що в сучасних умовах не існує єдиного загальноприйнятого підходу до оцінки ефективності систем захисту корпоративної інформації на підприємствах. Так, як справедливо відзначає колектив науковців, «ефективність функціонування комплексних систем захисту інформації залежить від безлічі взаємопов'язаних між собою елементів, що діють, і, як правило, оцінюються сукупністю критеріїв, що знаходяться в складних взаєминах. Відсутність на сьогоднішній день загального підходу до вирішення завдань даного класу закономірно спричиняє за собою різноманіття різних не взаємопов'язаних методів оцінки рівня захисту інформації» [6, с. 83].

Однією з проблем, які ускладнюють використання наявних в науковій літературі методик комплексної оцінки ефективності систем захисту інформації є складність способів згортки часткових показників, пропонованих у відповідних методиках, в інтегральний показник комплексної оцінки ефективності захисту інформації. Тож існує необхідність розробки більш простих у використання та наочних методик оцінки ефективності захисту інформації в межах функціонування відповідної системи. При цьому погоджуємося з авторами [6, с. 86], що цілком вірною є пропозиція оцінювати ефективність системи захисту корпоративної інформації, як складної системи і характеризувати її декількома частковими показниками, на підставі яких формується загальний критерій.

Тож першим кроком вважаємо за необхідне виділити окремі функціональні складові (підсистеми), за якими буде проводитися оцінка ефективності системи захисту корпоративної інформації в цілому. До вказаних складових віднесемо наступні:

– функціональна складова системи захисту корпоративної інформації, яка відображає рівень виконання функціональних обов'язків, навики, компетентність, управлінську ефективність працівників в сфері захисту інформації підприємства;

– економічна складова системи захисту корпоративної інформації, яка характеризує залежність результатів фінансово-господарської діяльності підприємства й витрат на захист інформації;

– організаційна складова системи захисту корпоративної інформації, яка відображає рівень ефективності організації матеріальних, нематеріальних й кадрових ресурсів в системі захисту інформації.

Наступним кроком в межах виділених функціональних складових визначимо сукупність показників, яка комплексно характеризуватиме рівень ефективності окремих підсистем захисту інформації та загальну ефективність системи захисту корпоративної інформації підприємства (табл. 1).

Як бачимо з табл. 1, для включення в пропоновану методику оцінки було обрано лише ті показники, які є стимуляторами, тобто для яких позитивною є тенденція до збільшення.

Щоб привести виділені по кожній складовій системи захисту корпоративної інформації підприємства

Таблиця 1

Система показників оцінювання ефективності системи захисту корпоративної інформації підприємства

Показник	Алгоритм розрахунку (економічна сутність показника)	Вагомість показника
Функціональна складова		
Коефіцієнт управлінських навиків в сфері захисту інформації	відношення досвіду роботи на посаді в сфері захисту інформації до загального стажу роботи на керівних посадах окремим працівником	0,10
Коефіцієнт повноти охоплення функцій захисту	відношення робіт, що фактично виконуються працівниками сфери захисту інформації, до робіт, що затверджені положеннями підприємства	0,20
Частка співробітників, що пройшли тренінги в сфері захисту інформації	відношення кількості працівників, які пройшли підвищення кваліфікації з проблем захисту інформації та інформаційної безпеки у мережах та ін. до загальної кількості працівників в системі захисту інформації підприємства	0,20
Коефіцієнт досвіду роботи персоналу	співвідношення чисельності працівників, маючих доступ до комерційної таємниці (баз чи банків даних тощо), що працюють на підприємстві більше одного року до загальної чисельності працівників, що мають доступ до комерційної таємниці (баз даних чи банків даних)	0,10
Коефіцієнт компетентності персоналу	співвідношення інформаційних загроз (інформаційних атак), які відвернуті через дії персоналу, який забезпечує захист інформації, до загальної кількості інформаційних атак за певний проміжок часу	0,25
Частка програмного забезпечення й технічних засобів, розроблених працівниками підприємства, яке задіяне для забезпечення захисту інформації підприємства	відношення кількості програмних і технічних заходів сфери захисту інформації, розроблених працівниками підприємства, до загальної кількості програмних і технічних заходів сфери захисту інформації, які використовуються на підприємстві	0,15
Економічна складова		
Коефіцієнт ефективності захисту інформації	відношення результату діяльності (чистого доходу, валового або чистого прибутку) до загальних витрат на захист інформації (включаючи витрати на програмні засоби захисту та контролю за використанням інформації, витрати на заробітну плату, витрати на судові процедури тощо)	0,20
Продуктивність праці в системі захисту інформації	відношення вартості виробленої продукції до кількості працівників, працюючих в сфері захисту інформації, чи обсягу відпрацьованого ними часу	0,10
Коефіцієнт прибутковості системи захисту інформації	відношення валового (чистого) прибутку до фонду оплати праці персоналу, задіяного в сфері захисту інформації	0,10
Коефіцієнт фінансування системи захисту інформації	відношення витрат підприємства на захист інформаційних ресурсів до загального розміру витрат підприємства	0,15
Коефіцієнт ефективності навчання	відношення чистого доходу (валового або чистого прибутку) до витрат на навчання персоналу в сфері захисту інформації	0,10
Відношення темпів приросту чистого доходу (валового або чистого прибутку) до темпів приросту витрат на захист інформації	відображає зміну доходу (прибутку) підприємства відносно зміни витрат підприємства на захист інформації	0,20
Відношення темпів приросту доходу (валового або чистого прибутку) до темпів приросту витрат на навчання персоналу в сфері захисту інформації	відображає зміну доходу (прибутку) підприємства відносно зміни витрат на навчання працівників в сфері захисту інформації	0,05
Відношення темпів приросту доходу (валового або чистого прибутку) до темпів приросту фонду оплати праці персоналу, задіяного в сфері захисту інформації	відображає зміну доходу (прибутку) підприємства відносно зміни витрат на оплату праці персоналу, задіяного в сфері захисту інформації	0,10
Організаційна складова		
Зайнятість персоналу в сфері захисту	відношення фактичної кількості працюючих до чисельності відповідно зі штатним розкладом	0,10
Рівень механізації та автоматизації праці персоналу в сфері захисту	відношення вартості основних засобів й не матеріальних активів, задіяних в сфері захисту, до чисельності працівників	0,10
Кількість загроз, що розпізнаються	визначає кількість загроз, що можуть розпізнаватися та оброблятися системою захисту інформації	0,25
Оперативність реагування системи захисту інформації на виявлені загрози	визначає дотримання системою захисту інформації підприємства стандартів часу	0,10
Коефіцієнт технічного захисту інформації	співвідношення кількості відвернутих інформаційних атак до загальної кількості інформаційних атак за певний проміжок часу	0,25
Коефіцієнт програмної захищеності інформації	співвідношення часу безперебійного функціонування системи захисту інформації до нормативного часу функціонування системи захисту інформації	0,20

Джерело: складено з урахуванням [1; 4; 5]

показники до порівняльного вигляду при розрахунку інтегральних показників оцінки ефективності системи захисту інформації підприємства пропонуємо розраховувати зважене значення показників (максимальному фактичному значенню показника за аналізований період присвоюється значення 1, зважені значення показників за інші роки в межах періоду аналізу знаходяться співвідношенням фактичного значення показника і-го року й максимального значення показника) й присвоювати вагомість кожному показнику оцінку (відображено в табл. 1).

Відзначимо, що для обґрунтування вагомості кожного з показників, включених до пропонованої методики оцінки ефективності системи захисту корпоративної інформації підприємства, було використано метод експертного оцінювання з використанням бальної шкали де максимальний бал відповідає найбільшій важливості показника, а мінімальний – найменшій (кількість балів залежить від кількості показників відповідної складової системи захисту корпоративної інформації).

Так, експертизу було проведено складом експертів із 10 осіб, якими виступили керівники середньої ланки промислових підприємств м. Київ та Київської області, з-поміж яких ПрАТ «Укргідроенерго» й ДП «Антонов». Кожному експерту було запропоновано розставити критерії важливості (бали) по кожному з оцінюваних коефіцієнтів. Фрагмент визначення вагомості показників оцінки ефективності функціональною складової системи захисту корпоративної інформації наведено в табл. 2.

Як бачимо з табл. 2, загальна сума балів, отриманих всіма коефіцієнтами, складає 210. Відповідно, вага кожного показника визначатиметься співвідношенням суми балів, отриманих кожних показником, на загальну суму балів.

Відзначимо, що за результатами експертного опитування спеціалістів було здійснено перевірку узгодженості думок експертів за допомогою коефіцієнту конкордації. Розрахований коефіцієнт конкордації за показниками оцінки ефективності кожної складової системи захисту корпоративної інформації підприємства засвідчив, що думки експертів є узгодженими, оскільки розрахункове значення коефіцієнту конкордації більше за нормативне (0,55). Так, коефіцієнт конкордації для наведеного в табл. 2 фрагменту дорівнює 0,708, отже коефіцієнт конкордації значущий, а думки експертів узгоджені. Аналогічно було розраховано вагові значення показників оцінки ефективності за іншими складовими системи захисту корпоративної інформації.

Інтегральний показник оцінки ефективності системи захисту корпоративної інформації у розрізі окремих складових (X_i) буде розраховано за формулою (1):

$$X_i = \sum_{i=1}^{n} K_i M_i \qquad (1)$$

де M_i – вагомість відповідного показника;

K_i – зважене значення показника в межах *i*-ї складової системи захисту корпоративної інформації підприємства.

Загальний інтегральний показник рівня ефективності системи захисту корпоративної інформації підприємства ($\overline{X}$) розраховується за формулою середньої геометричної (формула 2):

$$\overline{X} = \sqrt[3]{X_1 * X_2 * X_3}\,, \qquad (2)$$

де X_1, X_2, X_3 – значення інтегрального показника оцінки рівня ефективності системи захисту корпоративної інформації за відповідною складовою системи.

Позитивним рівень інтегрального показника оцінки ефективності системи захисту корпоративної інформації (та, відповідно, інтегральних показників її окремих складових) вважається тоді, коли значення інтегральних оцінок наближається до одиниці (табл. 3).

Таблиця 2

Фрагмент визначення вагомості показників оцінки ефективності функціональною складової системи захисту корпоративної інформації

Експерти	Показник					
	Коефіцієнт управлінських навиків в сфері захисту інформації	**Коефіцієнт повноти охоплення функцій захисту**	**Частка співробітників, що пройшли тренінги в сфері захисту інформації**	**Коефіцієнт досвіду роботи персоналу**	**Коефіцієнт компетентності персоналу**	**Частка програмного забезпечення й технічних засобів, розроблених працівниками підприємства**
1	1	5	4	2	6	3
2	3	5	6	1	4	2
3	1	4	6	3	5	2
4	2	1	5	3	6	4
5	4	6	2	1	5	3
6	1	3	6	2	5	4
7	1	5	3	4	6	2
8	3	1	4	2	6	5
9	2	6	3	1	4	5
10	3	5	4	2	6	1
Сума балів	21	41	43	21	53	31
Вага показника	= 21 / 210 = 0,10	= 41 / 210 = 0,20	= 43 / 210 = 0,20	= 21 / 210 = 0,10	= 53 / 210 = 0,25	= 31 / 210 = 0,15

Джерело: складено авторами

Таблиця 3

Шкала визначення рівня ефективності системи захисту корпоративної інформації підприємства за пропонованою методикою

Рівень ефективності	Значення інтегрального показника	Характеристика рівня ефективності системи захисту корпоративної інформації підприємства
Високий	0,80 і більше	Високий рівень ефективності системи захисту корпоративної інформації, що дає змогу забезпечити й підтримувати високий рівень інформаційної безпеки підприємства
Достатній	0,63–0,79	Рівень ефективності системи захисту корпоративної інформації підприємства перебуває в достатніх межах, що уможливлює мінімально необхідні і достатні параметри інформаційної безпеки підприємства. Однак, наявні окремі інформаційні небезпеки в процесі обміну, обробки та зберігання інформації у відповідних складових системи захисту корпоративної інформації підприємства
Середній	0,37–0,62	Рівень ефективності системи захисту корпоративної інформації недостатній для підтримання необхідних і достатніх параметрів інформаційної безпеки підприємства, проте існують можливості зміни параметрів функціонування системи захисту інформації на краще у разі зміцнення відповідних складових системи
Низький	0,2–0,36	Система захисту корпоративної інформації підприємства не забезпечує своєчасне реагування на виникнення й негативний вплив інформаційних ризиків та загроз й потребує модернізації.
Дуже низький	0–0,19	Рівень ефективності системи захисту корпоративної інформації генерує критичні загрози інформаційній безпеці й існуванню підприємства як соціально-економічної системи

Джерело: складено авторами

Відзначимо, що наведена у табл. 3 шкала є різновидом однієї з найбільш популярних в наукових економічних дослідженнях шкали бажаності Харрінгтона, яка досить часто використовується для інтерпретації інтегральних показників оцінки за різноманітними напрямами.

Висновки. Таким чином, було виділено основні складові системи захисту корпоративної інформації підприємства для кожної з яких побудовано систему показників оцінювання ефективності захисту інформації (обрано лише ті показники, які є стимуляторами для відповідного підприємства). З урахуванням виділених складових й пропонованих показників їх аналізу розроблено інтегральну методику оцінювання рівня ефективності системи захисту корпоративної інформації підприємства, яка передбачає розрахунок інтегрального показника за кожною визначеною складовою системи захисту інформації й загального інтегрального показника.

Запропонована методика оцінки ефективності системи захисту корпоративної інформації підприємства побудована на врахуванні взаємозв'язку сукупності виділених показників оцінки з ефективністю функціонування системи захисту інформації в умовах впливу зовнішніх та внутрішніх загроз та заснована на одному з базових принципів системного підходу, який передбачає, що кожна виділена складова системи захисту інформації, виконуючи відповідну функцію, забезпечує досягнення встановленої мети, якою є необхідний і достатній рівень ефективності захисту корпоративної інформації підприємства й, відповідно, його інформаційної безпеки.

Список використаних джерел:

1. Дячков Д.В. Методичні підходи до оцінки інформаційної безпеки підприємства. *Вісник Сумського національного аграрного університету. Серія «Економіка і менеджмент»*. 2017. № 12(74). URL: http://dspace.pdaa.edu.ua:8080/handle/123456789/2572 (дата звернення: 21.12.2021).

2. Кількість кіберзлочинів в Україні зросла вдвічі за останні п'ять років – Opendatabot. Mind. 21 жовтня 2019. URL: https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot (дата звернення: 23.12.2021).

3. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем. *Штучний інтелект*. 2008. № 4. С. 253–264.

4. Птіцина Л.А. Формування інформаційного забезпечення в системі управління підприємств хлібопекарської промисловості : дис. … канд. екон. наук : Спеціальність 08.00.04 – «Економіка і управління підприємствами» (за видами економічної діяльності). Запоріжжя : Запорізька державна інженерна академія, 2012. 263 с.

5. Сухорукова О.А. Напрями економічної оцінки інформаційної та інтелектуальної безпеки медіапідприємств. Science and education: trends and prospects : Collection of scientific articles. Ascona Publishing. New York, United States of America, 2018. P. 196–202.

6. Толюпа С.В., Самохвалов Ю.Я., Цьопа Н.В. Комплексні системи захисту інформації спеціальних об'єктів та методика їх оцінки. *Сучасний захист інформації*. 2014. № 1. С 81–88.

References:

1. Diachkov D. V. (2017) Metodychni pidkhody do otsinky informatsiinoi bezpeky pidpryiemstva [Methodical approaches to assessing the information security of the enterprise]. *Bulletin of Sumy National Agrarian University. Economics and Management*

Series (electronic journal), no. 12(74). Available at: http://dspace.pdaa.edu.ua:8080/handle/123456789/2572 (accessed 21 December 2021).

2. Mind (2021) Kilkist kiberzlochyniv v Ukraini zrosla vdvichi za ostanni piat rokiv – Opendatabot [The number of cybercrimes in Ukraine has doubled in the last five years – Opendatabot]. Available at: https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot (accessed 23 December 2021).

3. Maslova N. A. (2008) Metody otsenki effektivnosti sistem zashchity informatsionnykh sistem [Methods for assessing the effectiveness of information systems protection systems]. *Artificial Intelligence*, no. 4, pp. 253–264.

4. Ptitsyna L. A. (2012) *Formuvannia informatsiinoho zabezpechennia v systemi upravlinnia pidpryiemstv khlibopekarskoi promyslovosti* [Formation of information support in the management system of the bakery industry]. (PhD Thesis), Zaporozhye: Zaporozhye State Engineering Academy.

5. Sukhorukova O. A. (2018) Napriamy ekonomichnoi otsinky informatsiinoi ta intelektualnoi bezpeky mediapidpryiemstv [Directions of economic assessment of information and intellectual security of media enterprises]. Science and education: trends and prospects: Collection of scientific articles. Ascona Publishing, New York, United States of America, pp. 196–202.

6. Toliupa S. V., Samokhvalov Yu. Ia., Tsopa N. V. (2014) Kompleksni systemy zakhystu informatsii spetsialnykh obiektiv ta metodyka yikh otsinky [Comprehensive information protection systems for special objects and methods of their evaluation]. *Modern information protection*, no. 1, pp. 81–88.