Висновок або наукова новизна. Таким чином, економічний розвиток є однією з найголовніших цілей функціонування будь-якого підприємства, оскільки забезпечує задоволення нових потреб споживачів; підвищення конкурентоспроможності організації та зміцнення її позицій на міжнародній арені; створення умов та фінансово-технологічної бази для подальшого розвитку тощо. Власне, ефективне планування економічного розвитку може запровадити в організації нову стратегію і нову культуру, мобілізувати та сконцентрувати всю енергію й ресурси компанії на досягненні мети. Без належного планування в організації виникатимуть проблеми неефективного використання ресурсного потенціалу та наявних можливостей. [4]

Перспективою подальших досліджень є визначення економічних показників, які оцінюють та характеризують складові планування економічного розвитку, а також створення моделі планування економічного розвитку підприємства.

Перелік посилань:

1. Сергеев И. В. Экономика предприятия: Учеб. пособие для экон. спец. вузов / И. В. Сергеев. – 2-е изд., перераб. и доп. – Москва: Финансы и статистика, 2000. – 304 с.

2. Гринчуцький В. І. Економіка підприємства: навч. посібник / В. І. Гринчуцький, Е. Т. Карапетян, Б. В. Погріщук. – К.: Центр учбової літератури, 2010. – 304 с.

3. Нелеп В. М. Планування на аграрному підприємстві: Підручник. – 2-ге вид., перероб. та доп. – К.: КНЕУ, 2004. – 495 с.

4. Мала Н. Т., Грабельська О. В. Економічний розвиток підприємства: планування та моделювання [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/natural/Vnulp/Menegment/2012_739/04.pdf

Стаття надійшла: 12.09.2016 р.
Рецензент: д.е.н., проф. Іванілов О.С.

УДК : 004.056.5
JEL classification : D 800

ОСНОВИ ФОРМУВАННЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Маркіна І.А., д.е.н. , професор
Дячков Д.В., к.е.н.
Полтавська державна аграрна академія

Анотація. *У статті розглянуто передумови формування системи інформаційної безпеки підприємства та визначено особливості управління нею, що пов'язані з постійним розвитком інформаційної інфраструктури підприємства, наданням різних видів інформаційних сервісів, автоматизації фінансової та виробничої діяльності, а також бізнес-процесів сучасної організації. Визначено дуальність поглядів на процес формування системи інформаційної безпеки підприємства: які, з однієї сторони – обумовлені обов'язковістю виконання вимог стандартів, нормативів, процесів ліцензування, тощо; з іншого – розумінням власника або вищого керівництва організації необхідності впровадження системи захисту інформації. Тому метою статті стало визначення вимог до формування ефективної моделі інформаційної безпеки підприємства та аналіз особливостей її формування.*

Відповідно до встановленої мети розглянуто та охарактеризовано основні драйвери формування системи інформаційної безпеки підприємства, серед яких провідне місце займають: необхідність відповідності різним нормативним актам, а також захист приватних та корпоративних даних.

На основі проведеного аналізу сучасних підходів до визначення сутності інформаційної безпеки, на основі узагальнення теоретичних положень та досвіду функціонування організацій запропоновано систему інформаційної безпеки підприємства розглядати як модель інформаційного протиборства з факторами внутрішнього та зовнішнього середовища.

Відповідно, елементом новизни стало формування моделі системи менеджменту інформаційної безпеки підприємства на основі ризик-орієнтованого підходу з врахуванням рекомендацій ISO / IEC 27003 «Information technology – Security techniques – Information security management system implementation guidance». Запропоновано етапи формування системи менеджменту інформаційної безпеки суб'єкту господарювання, що об'єднуються за трьома основними напрямами: встановлення сфери застосування і політики системи менеджменту інформаційної безпеки підприємства, вибір захисних заходів на основі системи ризик-менеджменту та отримання схвалення керівництва для впровадження засобів та форму-

вання заходів обробки ризиків та формулювання рівня можливості застосування вимог з каталогів вимог вітчизняних та міжнародних стандартів.

Ключові слова: *захист інформації, інформаційна безпека, стандарти, система менеджменту інформаційної безпеки, ризик-менеджмент, загрози, інформаційні системи.*

BASIS OF FORMATION ENTERPRISE'S MANAGEMENT INFORMATION SECURITY SYSTEM

Dr. Iryna Markina, DS in Economics, Professor
Poltava State Agrarian Academy
Dmytro Dyachkov, PhD in Economics, Associate Professor
Poltava State Agrarian Academy

Summary. *The article considers the preconditions of enterprise information security and the control features are defined by it, that associated with the continuous development of enterprise information infrastructure, the provision of various types of information services, automation of financial and operational performance, as well as the business processes of modern organizations. It is determined the duality of views on the process of formation of the information security system of the enterprise: that on the one hand - due to the mandatory implementation of the requirements of standards, regulations, licensing, etc .; on the other - an understanding of the owner or senior management of the organization need to implement information security systems. Therefore, the purpose of the article is to define the requirements for the formation of an effective information security and business model analysis of the peculiarities of its formation.*

According to the stated goal there were reviewed and characterized the main drivers of formation of information security companies, among them the leading place belongs to: the need for compliance with different regulations, and the protection of private and corporate data.

The proposed enterprise information security system is regarded as a model of information warfare with the factors of internal and external environment, based on the analysis of modern approaches to the definition of information security, and on a synthesis of theoretical positions and experience of functioning of the organizations

Accordingly, the element of novelty is the creation of an information security management system model of the enterprise on the basis of risk-based approach taking into account the recommendations of the ISO / IEC 27003 «Information technology - Security techniques - Information security management system implementation guidance». There ere proposed the stages of formation of the information security management system of the business entity, which combine for three main areas: establishing the scope and policies of information security management system of the enterprise, the choice of protective measures on the basis of the risk management system and obtaining management approval for implementation of funds and the formation of risk treatment measures and formulating level of the possibility of applying the requirements of the catalog of requirements of domestic and international standards.

Keywords: *protection of information, information security, standards, management system of information security, risk management, threat, information systems.*

Постановка проблеми. Процес успішного функціонування розвитку підприємства залежить від прийняття якісних і своєчасних управлінських рішень, які формуються на основі ретельного та всебічного аналізу інформації, що надходить як з внутрішнього, так і з зовнішнього середовища. В останні десятиліття, у зв'язку з розвитком інформаційних технологій і загальною інформатизацією соціально-економічних відносин зросло значення інформації не тільки для економіки, але і для суспільства в цілому. Інформація стала одним з найбільш важливих управлінських ресурсів, нарівні з людськими, фінансовими і матеріальними. З підвищенням ролі інформації, сформувався інформаційний простір, який вимагає захисту від несанкціонованого або, навіть, ненавмисного впливу на рівні держави, регіону, і навіть на рівні окремих підприємств. В економічній діяльності захист інформації дає можливість отримувати високі доходи, укладати вигідні контракти з контрагентами, що істотно підвищує рівень конкурентоспроможності підприємства, а також дозволяє значно підвищити ефективність діяльності організації в цілому.

Сучасні інформаційні системи призначені для забезпечення працездатності інформаційної інфраструктури підприємства, надання різних видів інформаційних сервісів, автоматизації фінансової та виробничої діяльності, а також бізнес-процесів організації, що дозволяють скоротити як фінансові, так і трудові витрати. В інформаційних системах зберігаються і обробляються значні обсяги інформації різного ступеня секретності, тому гостро постає питання про захищеність цих інформаційних систем підприємства від різних загроз безпеці інформації.

Зазначені передумови визначають провідну роль формування системи інформаційної безпеки підприємства та визначення особливостей управління нею.

Аналіз останніх досліджень і публікацій. Питанням формування системи інформаційної безпеки підприємства присвячені праці Андріанова В. В. [1], Гладких А. А. [2], Гатчин Ю. А, Климової Є. В. [3], Моїсеєва А.І. [4], Ромака В.А. [5] та інших.

Вітчизняна і світова практика формування системи інформаційної безпеки підприємства, управління нею свідчать про дуалістичність поглядів на цей процес: з одного боку – обов'язкових вимог національних уповноважених органів (стандарти, нормативи, процеси ліцензування) [6-10], з іншого – розуміння власника або вищого керівництва організації відносно необхідності впровадження комплексів захисту інформації. Тому, для менеджменту і власників існувала головна проблема – відповідність встановленим вимогам до захисту інформації, та головний спосіб її вирішення – як з мінімальними витратами виконати встановлені вимоги. Для уповноважених органів проблема полягала в наступному: яким чином в силу неможливості охоплення всіх можливих видів діяльності і умов їх реалізації, а також істотних відмінностей в цілях діяльності організацій запропонувати універсальний набір вимог щодо формування систем інформаційної безпеки. Як наслідок, інформаційна безпека розглядалася як самодостатня сутність, інваріантна до діяльності, цілей, умов, а також істотно звужувалась в змістовності для досягнення універсальності [1, 2, 5].

Невирішені складові загальної проблеми. Розглянуті підходи визначення сутності системи інформаційної безпеки підприємства (організацій і регуляторів) є невідповідними існуючим реаліям господарювання та характеризують її у викривленому вигляді. Так, основні змістовні обмеження щодо діяльності із забезпечення інформаційної безпеки пов'язані з традиційною моделлю інформаційної безпеки, яка передбачає обов'язкову наявність зловмисника, що прагне завдати шкоди активам (інформації), і, відповідно, технічної та програмної частин орієнтованих на захист інформації від дій такого суб'єкта (групи суб'єктів). При цьому інциденти, пов'язані, наприклад, зі штатними змінами прикладного софту, порушення процедур роботи з інформацією персоналом підприємства, низький рівень забезпеченості технічними засобами та інше, не можуть бути віднесені до дій зловмисника. Їх головні причини – низькоефективний менеджмент і невідповідна програмно-технологічна база. Власне, неефективність менеджменту підприємств, відсутність органів управління системою інформаційної безпеки на підприємстві являє собою потужне джерело проблем, які ігноруються в силу неможливості їх прив'язки до дій зловмисника.

Поступове усвідомлення факту, що інформаційний вплив на бізнес-процеси, на управління ними може бути ефективніший, ніж вплив інших факторів перетворюють інформаційне протиборство в головний інструмент виживання і конкурентної боротьби. А це, в свою чергу, виводить на перший план роль інформаційної безпеки, яка повинна бути інтегрована в бізнес-процеси.

Формулювання цілей статті. Метою статті є визначення вимог до формування ефективної моделі інформаційної безпеки підприємства та аналіз особливостей формування ефективної системи менеджменту інформаційної безпеки.

Виклад основного матеріалу дослідження. Важливим аспектом дослідження системи управління інформаційною безпекою є визначення сучасного розуміння інформаційної безпеки, її значення для реалізації основних бізнес-процесів.

Аналіз наопрацювань вітчизняних та зарубіжних науковців надав змогу визначити, що найбільш розповсюдженим є визначення інформаційної безпеки як певного рівня захищеності інформації від незаконного ознайомлення, перетворення і знищення, а також захищеність інформаційних ресурсів від впливів, спрямованих на порушення їх працездатності. Природа цих впливів може бути найрізноманітнішою. Це і спроби проникнення зловмисників, і помилки персоналу, і вихід з ладу апаратних і програмних засобів, стихійні лиха тощо [1, 2, 4, 11].

Інша група науковців, з точки зору бізнесу, під інформаційною безпекою підприємства розуміють стан захищеності інтересів (цілей) організації в умовах загроз в інформаційній сфері. На їх думку, інформаційна сфера є сукупністю інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, розповсюдження, зберігання і використання інформації, а також системи регулювання виникаючих при цьому відносин [5, 12, 13].

Відповідно до вищезазначених підходів, відповідь на питання про роль інформаційної безпеки в бізнесі сучасної організації є очевидною, оскільки підприємства розг-

лядали її як «звичайну страховку» від проблем і неприємностей: «…заплатив гроші, впровадив рішення і можеш спокійно зосередитися на основній діяльності…» [14].

Однак розвиток ринку, інформатизація сфер діяльності суб'єктів господарювання, зростання кількості загроз і засобів забезпечення безпеки призводить до принципово іншого розуміння ролі інформаційної безпеки. В умовах глобальної інформатизації її не можна сприймати виключно як захист або «страховку» – вона переростає в більше, а саме – в один з ключових бізнес-активів сучасної організації. На думку фахівців аналітичного центру компанії Perimetrix, впровадження технологій інформаційної безпеки може сприяти зростанню прибутковості або загальної ефективності бізнесу безпосередньо, а не тільки за рахунок мінімізації ризиків [14].

За даними дослідження Ernst & Young послуг, основними драйверами (причиною використання рішень) сучасного ринку інформаційної безпеки (рис. 1) для 67% респондентів є необхідність відповідності різним нормативним актам.

Цей пункт очолює список з 2005 року [15]. Цікаво, що до 2005 року серед факторів, що стимулюють розвиток інформаційної безпеки, перше місце займали технічні загрози, класичні віруси і мережеві «черв'яки». При цьому більшість нормативних актів впливають на інформаційну безпеку опосередковано. Так, наприклад, основна мета закону SOX – забезпечити прозорість внутрішнього контролю і коректність інформації в звітах, а завдання нормативу Basel II – спонукати фінансові компанії резервувати операційні ризики. Ні той, ні інший не стосуються інформаційної безпеки безпосередньо, проте, здійснюють на неї значний вплив, причому. За інформацією Ernst & Young, в цілому 80 % опитаних вважають, що відповідність нормативним актам позитивно впливає на інформаційну безпеку.

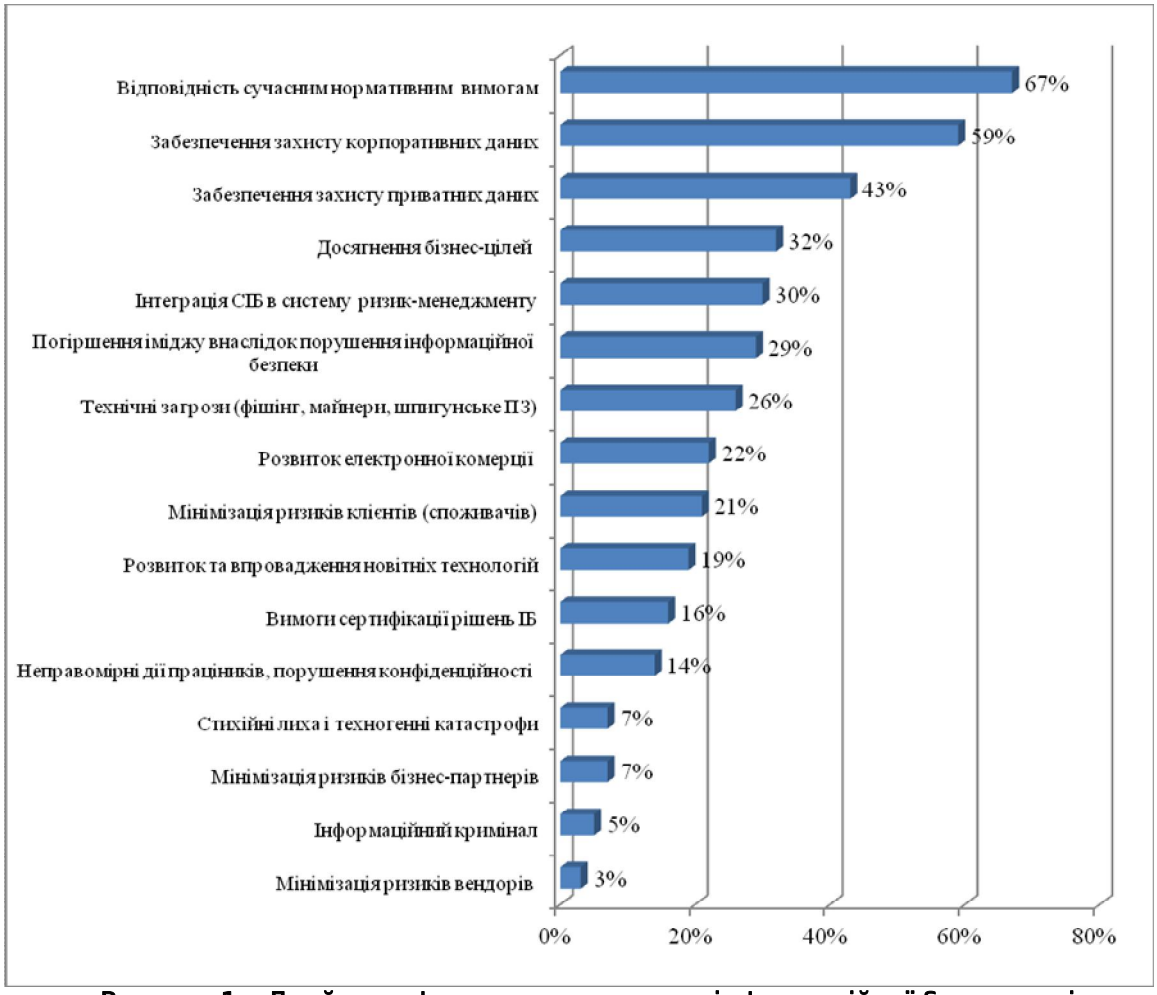

Рисунок 1 – Драйвери формування системи інформаційної безпеки підприємства [3, 12, 14, 15]

Фахівці аналітичного центру компанії Perimetrix вважають дане питання надзвичайно актуальним і для українських підприємств.

За даними різних досліджень, більшість вітчизняних фахівців позитивно оцінюють вплив Конституції України [16], Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [6], Закону України «Про захист персональних даних» [7], Постанови КМУ «Про затвердження Концепції технічного захисту інформації в Україні» [8], Постанови КМУ «Про прийняття за основу проекту Закону України «Про Концепцію державної інформаційної політики [9] на інформаційну безпеку.

Позитивною тенденцією формування та впровадження системи інформаційної безпеки на підприємстві є захист приватних та корпоративних даних – 43 % і 59 % відповідно.

Найменш значними драйверми формування системи інформаційної безпеки на підприємстві є мінімізація ризиків вендорів, протистояння інформаційному криміналу, мінімізація ризиків бізнес-партнерів, стихійні лиха та техногенні катастрофи.

Відповідно до вищезазначеного систему інформаційної безпеки підприємства пропонується розглядати як модель інформаційного протиборства з впливом факторів внутрішнього та зовнішнього середовища. Зміст інформаційного протиборства включає дві складові частини, які охоплюють сукупність дій, що дозволяють отримати інформаційну перевагу (рис. 2).

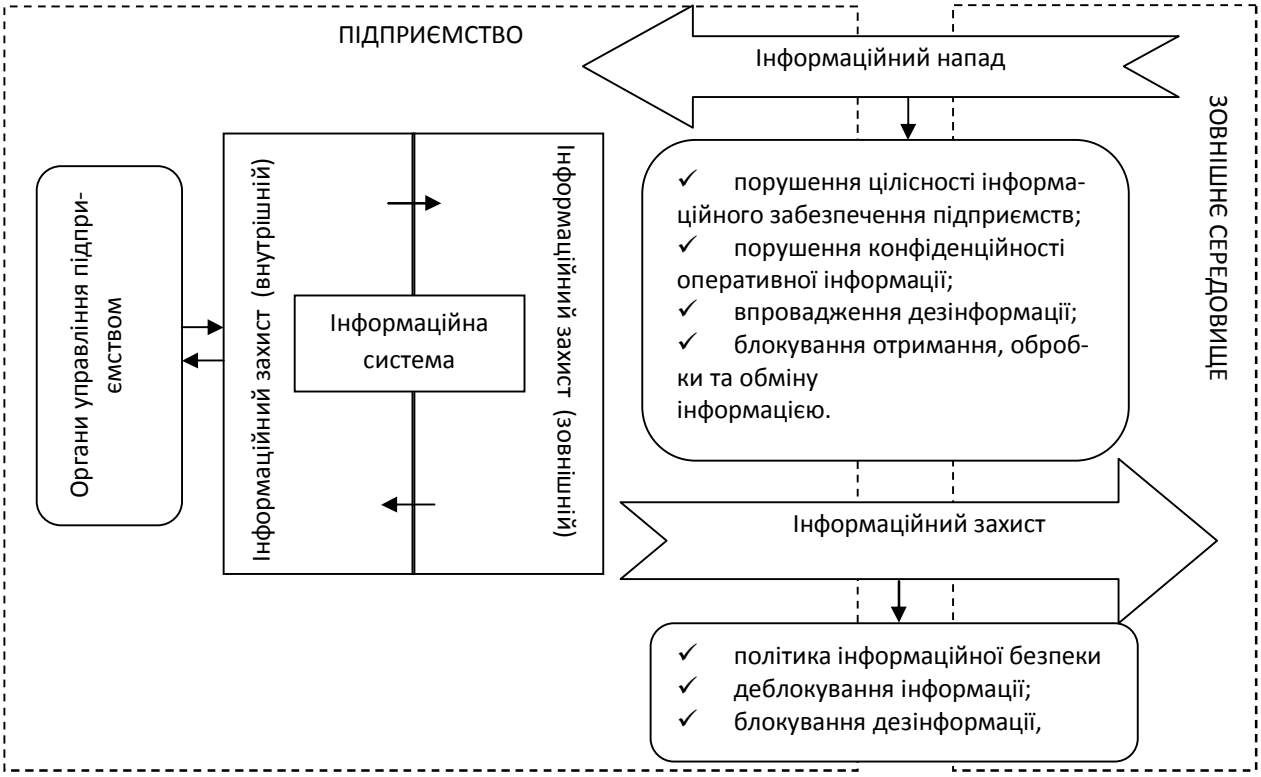

Рисунок 2 – Структура моделі інформаційного протиборства підприємства

Першою складовою (інформаційний напад) є протидія порушення цілісності інформаційного забезпечення підприємства з боку зовнішнього середовища, що включає заходи щодо порушення конфіденційності оперативної інформації, дезінформацію, блокування отримання даних, відомостей, обробки та обміну інформацією (включаючи фізичне знищення носіїв інформації) та блокування фактів дезінформації на всіх етапах інформаційного забезпечення управління. Інформаційна протидія здійснюється шляхом проведення комплексу заходів, що включають технічну розвідку систем зв’язку і управління, перехоплення інформації каналами зв’язку.

Друга частина (інформаційний захист) включає заходи щодо захисту інформації підприємства, засобів її зберігання, обробки, передачі та автоматизації захисту цих процесів від зовнішніх впливів (інформаційний захист), що передбачає визначення інформаційної політики, дії по деблокуванню інформації (в тому числі захист носіїв інформації від фізич-

ного знищення), необхідної для вирішення завдань управління, блокування дезінформації, яка розповсюджується і впроваджується в систему управління підприємства.

Розглянуті підходи до визначення інформаційної безпеки, визначені драйвери формування системи інформаційної безпеки підприємства та модель інформаційного протиборства обумовлюють доцільність формування системи менеджменту інформаційної безпеки на основі ризик-орієнтованого підходу, який ґрунтується на припущенні того, що оцінка ризику робить можливим вирішення питань, пов'язаних з інформаційними активами організації: актуальні загрози і їх джерела – фактори ризику; можливість і періодичність виникнення загроз; визначення інформаційних активів (їх кількісний аналіз), які можуть підлягати впливу при виникненні загрози [1].

Аналіз напрацювань в даній сфері дозволив визначити, що стандартній системі управління інформаційною безпекою підприємства притаманні всі загальні для систем менеджменту елементи. При цьому досвід використання стандартизованих вимог до системи менеджменту інформаційної безпеки визначив основні фактори для забезпечення інформаційної безпеки на сучасному підприємстві:

- політика інформаційної безпеки, цілі та заходи, що відображають цілі бізнесу суб'єкта господарювання;
- підхід і структура реалізації, підтримки моніторингу та вдосконалення інформаційної безпеки, узгоджуються з культурою організації;
- підтримка і прихильність керівництва всіх рівнів;
- розуміння вимог інформаційної безпеки, оцінка ризику та наявність ризик-менеджменту;
- ефективні заходи щодо формування компетентності з питань інформаційної безпеки для належного усвідомлення;
- поширення настанов (інструкцій) з політики та стандартів інформаційної безпеки серед всіх керівників, службовців та інших контрагентів;
- забезпечення фінансування заходів менеджменту інформаційної безпеки;
- забезпечення відповідної інформованості, навчання і освіти;
- встановлення ефективного процесу менеджменту інцидентів інформаційної безпеки;
- оцінювання системи, яке використовується для оцінки ефективності функціонування менеджменту інформаційної безпеки і пропозицій щодо вдосконалення.

Реалізація системи менеджменту інформаційної безпеки підприємства (СМІБ) може бути організована як сукупність управління цільовими (профільними) процесами діяльності, що ініціюються і завершуються за прийнятими для них критеріями (за часом або подією) (рис. 3).

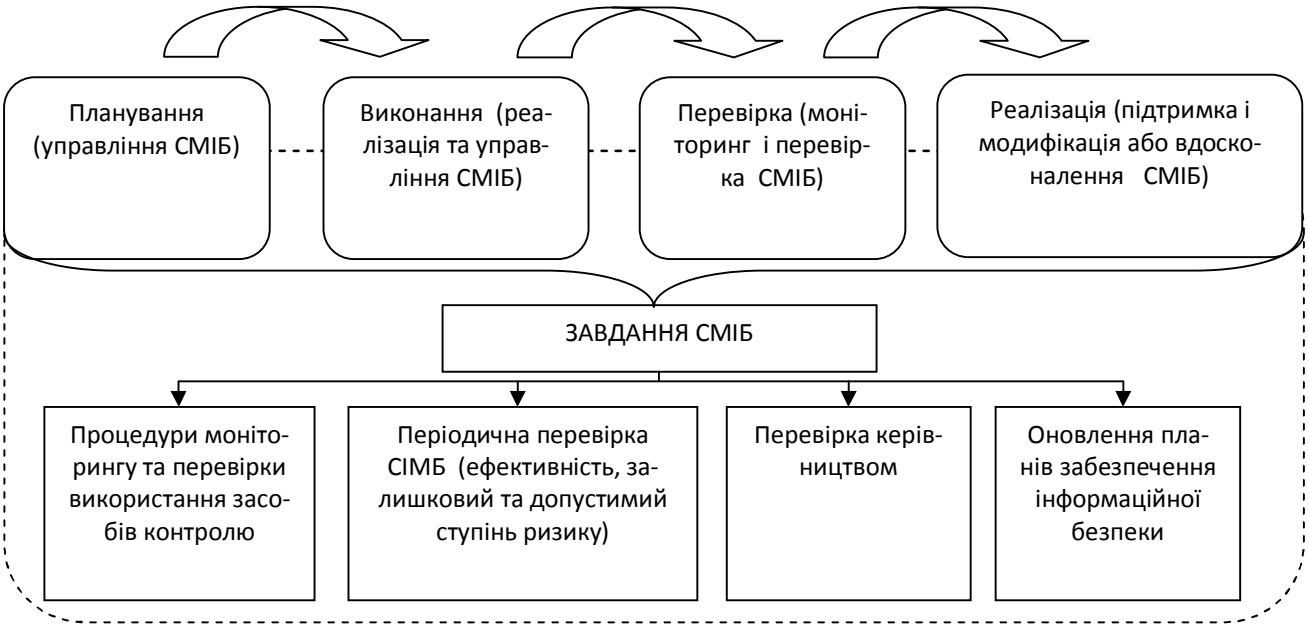

Рисунок 3 – Модель системи менеджменту інформаційної безпеки підприємства
[розроблено на основі 1]

Потрібно враховувати, що тільки вище керівництво підприємства повинно мати повноваження по визначенню рівня (порогів) ризиків в сфері забезпечення інформаційної безпеки, які є специфічними для кожної організації. Це обумовлено тим, що саме керівництво несе остаточну відповідальність за інвестиції в систему менеджменту інформаційної безпеки та її ефективність.

Тому не менш важливу роль у формуванні зазначеної системи відіграє дотримання вимог державних та міжнародних нормативно-правові актів і стандартів в даній сфері. За цих умов стандарти виступають в якості можливого еталона дій, але не як незмінна константа. Керівництво знаходиться, в деякому сенсі, в багатовимірному просторі, де повинно зорієнтуватися, оцінити кожен вектор і прийняти необхідне рішення відносно дотримання стандартів та положень інформаційної безпеки.

Як було зазначено, вітчизняні нормативно-правові акти та стандарти носять більш декларативний характер і не враховують специфіку інформатизації діяльності окремих суб'єктів господарювання. Водночас, практично всі міжнародні стандарти системи менеджменту методологічно сумісні, що дозволяє виділяти і підтримувати уніфіковані завдання, наприклад, в частині роботи з персоналом організації відносно користування інформацією та її захистом, реєстрації та збору інформації, формування інформаційних систем, використання засобів автоматизації тощо.

В такому випадку, процедури для реалізації і управління системою менеджменту інформаційної безпеки можуть бути організовані як дерево процесів. При прийнятті підприємством рішення про вибір підходу щодо формування системи менеджменту інформаційної безпеки доцільно враховувати рекомендації під: ISO / IEC 27003 «Information technology – Security techniques – Information security management system implementation guidance» [10]. Положення даного міжнародного стандарту ґрунтуються на методології процесного підходу, включаючи специфікацію всіх формальних атрибутів можливих процесів системи менеджменту інформаційної безпеки [10]. Питання реалізації системи менеджменту інформаційної безпеки на практиці невіддільні від відповідних процедур контролю, організованих в окремому блоці вимог системи менеджменту інформаційної безпеки.

Відповідно до пропонованої моделі системи менеджменту інформаційної безпеки головними завданнями органів управління виступають моніторинг та контроль. Формально, зміст робіт контролю інформаційної безпеки підприємства повинен включати:

- здійснення моніторингу та перевірка процедур та інших засобів контролю ризиків (захисних заходів) для швидкого виявлення помилок в результатах обробки, швидкої ідентифікації порушень безпеки, надання керівництву інформації, сприяння виявленню подій небезпеки і запобігання виникнення інцидентів загроз інформаційній та іншим видам безпеки підприємства за допомогою використання відповідної системи критеріїв;
- регулярні перевірки ефективності системи менеджменту інформаційної безпеки (включаючи дотримання політики і досягнення цілей системи менеджменту інформаційної безпеки, перевірку засобів контролю безпеки), враховуючи результати аудитів безпеки, інцидентів, результати вимірювань ефективності, пропозиції усіх зацікавлених сторін;
- перегляд оцінки рівня ризику через заплановані інтервали часу, а також визначення залишкових ризиків та ідентифікація прийнятних рівнів ризику відповідно до змін в організації та в її операційному і бізнес-середовищі;
- здійснення внутрішніх аудитів діяльності системи менеджменту інформаційної безпеки;
- здійснення перевірки керівництвом системи менеджменту інформаційної безпеки для підтвердження адекватності сфери її дії і ефективності заходів щодо вдосконалення системи менеджменту інформаційної безпеки, тощо.

У загальному випадку послідовність формування ефективної системи менеджменту інформаційної безпеки та завдань може включати наступні 10 етапів, реальне наповнення яких визначається самим підприємством (рис. 4).

Фактично представлені етапи формування системи менеджменту інформаційної безпеки мають на меті прийняття рішення за такими основними напрямами:

- встановлення сфери застосування і політики системи менеджменту інформаційної безпеки підприємства (етапи 1-2);
- вибір захисних заходів на основі системи ризик-менеджменту (етапи 3-7);

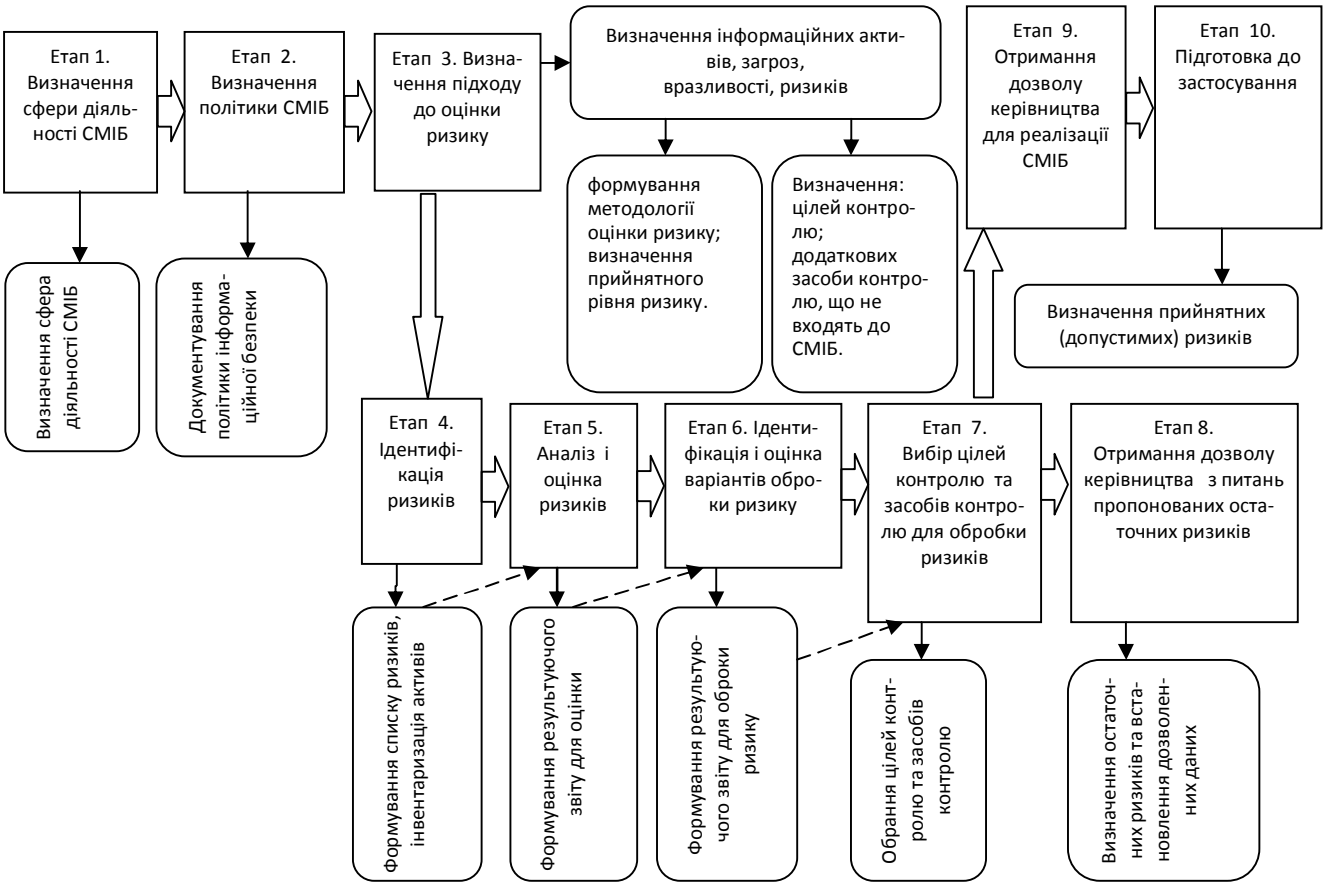

Рисунок 4 – Послідовність формування системи менеджменту інформаційної безпеки суб'єкту господарювання *[розроблено на основі 1, 2, 4]*

– отримання схвалення керівництва для впровадження засобів та формування заходів обробки ризиків; формулювання рівня можливості застосування вимог з каталогів вимог вітчизняних та міжнародних стандартів формування ефективної системи менеджменту інформаційної безпеки підприємства, що передбачає організаційні, фінансові витрати (етапи 8-10).

При встановленні сфери застосування і політики системи менеджменту інформаційної безпеки повинні розглядатися: стратегічні питання бізнесу, організаційні аспекти, місце розташування (географічне і фізичне), активи (в тому числі, інформаційні), технології.

Висновок. Таким чином управління інформаційною безпекою є невід'ємною частиною корпоративного управління підприємством, що мають як загальні фактори: об'єкти, предмети, зв'язки, так і відмінності. Досвід, накопичений в останні десятиліття, переконує в необхідності застосування міжнародних модельних стандартів формування системи менеджменту інформаційної безпеки вітчизняного підприємства, що має базуватися на ризик-орієнтованому підході управління інформаційними технологіями. Проте, на практиці реалізація політики інформаційної безпеки суб'єктів господарювання ускладнюється пошуком компромісу між відповідністю, зручністю і безпекою. Тому наступним напрямом дослідження стане аналіз методичних підходів до визначення рівня інформаційної безпеки підприємства.

Перелік посилань:

1. Андрианов В. В. Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. – М. : ООО «Альпина», 2010 – 265 с.

2. Гладких А. А. Базовые принципы информационной безопасности вычислительных сетей : учебное пособие для студентов, обучающихся по специальностям 08050565, 21040665, 22050165, 23040165 / А. А. Гладких, В. Е. Дементьев – Ульяновск : УлГТУ, 2009. – 156 с.

3. Инсайдерские угроы в России '14. [Электронный ресурс]. – Режим доступа : http://www.perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_in _Russia_2014.pdf

4. Моисеев А. И. Информационная безопасность распределённых информационных систем : учеб. / А. И. Моисеев, Д. Б. Жмуров. – Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2013. – 180 с.

5. Ромака В. А. Менеджмент у сфері захисту інформації / В. А. Ромака, Р. О. Корж, Ю. Р. Гарасим. – Львів : ЗУКЦ, 2013. – 462 с.

6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України, Верховна Рада України; Закон від 05.07.1994 № 80/94-ВР. [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show /80/94-вр

7. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – Ст. 481.

8. Про затвердження Концепції технічного захисту інформації в Україні: Постанова КМ України [Електронний ресурс]. – Режим доступу : http://zakon2. rada.gov.ua.

9. Про прийняття за основу проекту Закону України «Про Концепцію державної інформаційної політики» : Постанова Верховної Ради України від 11.01.2011 № 2897-VI [Електронний ресурс]. – Режим доступу: http://zakon1. rada.gov.ua.

10. ISO/IEC 27003 : 2010 Information technology — Security techniques — Information security management system implementation guidance. [Electronic resource]. – Access mode : https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-1:v1:en

11. Безопасность информационного пространства : сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных / сост. А.Н. Соколов. – Челябинск : Издательский центр ЮУрГУ, 2015. – 246 с.

12. Гатчин Ю. А., Климова Е. В. Основы информационной безопасности: учебное пособие. – СПб : СПбГУ ИТМО, 2009. – 84 с.

13. Лагун А. Ризики інформаційної безпеки ІТ-підприємства / А. Лагун, Н. Кухарська // [Електронний ресурс]. – Режим доступу : http://www.google. com.ua/url?url=http://sci.ldubgd.edu.ua:8080/bitstream/handle/123456789/750/11.doc%3Fsequence%3D1%26isAllowed%3Dy&rct=j&q=&esrc=s&sa=U&ved=0ahUKEwjz_823xfrPAhVB2SwKHbpaA5wQFggZMAE&usg=AFQjCNGlfE5rDW5CCFrQNLL5Ha42UVvO3g

14. Perimetrix. [Електронний ресурс]. – Режим доступу: http://www. perimetrix.com/

15. Ernst & Young. Британская аудиторско-консалтинговая компания. [Електронний ресурс]. – Режим доступу: http://www.ey.com/ua/uk/home

16. Конституція України від 28 червня 1996 р. № 254к/96-ВР [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua.

Стаття надійшла: 08.10.2016 р.
Рецензент: д.е.н., проф. Дмитрієв І.А.

УДК 330.356.7.002.6
JEL Classification: C610

ОПТИМАЛЬНА ФОНДООЗБРОЄНІСТЬ І ОЦІНКА ЗОН БЕЗЗБИТКОВОГО ІНВЕСТУВАННЯ НА БАЗІ ВИРОБНИЧИХ ФУНКЦІЙ

Янковий В. О., к.е.н.
Одеський національний економічний університет

Анотація. *Розглядаються теоретичні та практичні питання економічної науки, що пов'язані з визначенням оптимального поєднання ресурсів у рамках виробничих функції Кобба-Дугласа та функції з постійною еластичністю заміщення факторів. Наводяться формули оптимальної фондоозброєності для вказаних моделей, а також нерівності, які забезпечують беззбитковість інвестування у виробництво, що адекватно описується функціями Кобба-Дугласа, Кобба-Дугласа-Тінбергена.*

На основі диференційного аналізу функції з постійною еластичністю заміщення факторів виводяться зони беззбиткового інвестування у виробництво для трьох випадків у залежності від значення показника ступеня однорідності функції. При цьому передбачається виконання умови про здійснення капіталовкладення у виробничі фонди і робочу силу в пропорції, що відповідає оптимальній фондоозброєності.

Відзначається, що виконання виведених нерівностей прямо залежить від величини коефіцієнта шкали функції з постійною еластичністю заміщення факторів. Малі значення даного параметра, отримані в економіко-математичному дослідженні, сигналізують про негативний стан економіки підприємства (галузі, регіону, країни), в першу чергу, за рахунок недосконалості законодавства і податкової політики держави. Саме переважно фіскальний характер існуючої податкової політики держави по відношен-