УДК 65.012.8

МЕТОДИЧНІ ПІДХОДИ ДО ОЦІНКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Дячков Д.В., к.е.н., Полтавська державна аграрна академія

У статті визначено актуальність дослідження методичних підходів до оцінки інформаційної безпеки підприємства. Важливість цього напрямку дослідження полягає, перш за все, в обґрунтуванні необхідності формування комплексної системи діагностики рівня інформаційної безпеки та кількісної і якісної оцінки стану рівня інформаційної захищеності підприємства.

Проведений аналіз дозволив визначити два основних підходи до оцінки інформаційної безпеки підприємства: перший заснований на характеристиці захисних для об'єкта оцінки механізмів і достатності системи захисту; другий підхід заснований на тісному зв'язку системи показників кількісних оцінок інформаційної безпеки з ефективністю функціонування інформаційної системи в умовах впливу всіх видів загроз інформаційної безпеки.

На основі узагальнення форм, методів та підходів запропоновано систему показників оцінки інформаційної безпеки, яка базується на основних напрямах захисту інформації та враховують: оцінці програмно-технічної захищеності інформації, оцінці витрат на забезпечення інформаційної безпеки, оцінці інформаційної надійності персоналу, оцінку інформації, що надається особам, які приймають рішення, інформаційною службою підприємства, оцінці ризику, надійності, гнучкості та керованості системи захисту інформації.

Ключові слова: *загрози, інформаційна безпека, методичний підхід, оцінка інформаційної безпеки, показники, програмно-технічний захист, управління системою інформаційної безпеки.*

Постановка проблеми у загальному вигляді. Сучасні інформаційні технології та інформаційні системи активно впроваджуються в усі сфери національної економіки. В умовах глобалізації економіки, успішне ведення бізнесу передбачає наявність зовнішньої та внутрішньої інформації. Така інформація повинна відповідати вимогам актуальності, достовірності, структурованості, конфіденційності. Практика діяльності господарюючих суб'єктів повсякденно свідчить про їх підвищену вразливість від незаконних та інших посягань злочинних організацій та окремих осіб з метою викрадення інформаційних ресурсів, псування програмного та техніко-технологічного забезпечення, розкриття

комерційної таємниці підприємства тощо. Ускладнення засобів, методів, форм автоматизації процесів обробки інформації підвищує залежність підприємств від ступеня безпеки використовуваних ними інформаційних технологій, при цьому якість інформаційної підтримки управління безпосередньо залежить від організації інфраструктури захисту інформації. Тобто, проблема забезпечення інформаційної безпеки сучасних підприємств стоїть у ряді перших і найважливіших. Важливість цього напрямку полягає, перш за все, в обґрунтуванні необхідності формування комплексної системи діагностики рівня інформаційної безпеки та кількісної і якісної оцінки стану рівня інформаційної захищеності підприємства.

Аналіз останніх досліджень та публікацій. Питанням формування критеріїв та показників оцінки рівня інформаційної безпеки розглядалися в міжнародних та вітчизняних стандартах та нормативах, а також праці їх присвячені праці як вітчизняних, так і зарубіжних фахівців в області захисту інформаї, зокрема: Андріанов В. В. [5], Велігура А. В. [6], Врублевский К. Е. [12], Голдуєв Н. А. [5], Голованов В. Б. [5], Грибков С. В. [9], Журавель М. Ю. [7], Зефіров С. Л. [5], Ілляшенко С.М. [8], Кононова В. О. [9], Кравчук О. Я. [10], Кравчук П. Я. [10], Максименко В. Н. [11], Морозова В.І. [12], Полозова Т. В. [7], Реверчук Н. Й. [13], Стороженко О. В. [7], Харкянен О. В. [9], Хоффман Л. Дж. [14], Ясюк Е. В.[11] та ін. У працях присвячених оцінки рівня захисту інформації зазначених та інших фахівців найчастіше виявляється, що погляди в цій області суттєво різняться, іноді майже до протилежних. А відтак, відсутність комплексності в основних методичних підходах до діагностики ступеня інформаційної безпеки, в яких науковці намагаються інтегрувати існуючі положення, найбільш повно врахувати критерії та показники оцінки інформаційної безпеки, обумовлює необхідність формування універсальної системи оцінки рівня інформаційної захищеності підприємства.

Формування цілей статті. Метою статті визначено проведення аналізу методичних підходів до оцінки інформаційної безпеки підприємства та розробка концептуальних основ комплексної універсальної системи оцінки рівня інформаційної безпеки підприємства.

Виклад основного матеріалу. Якість та ефективність функціонування інформаційної системи визначається рівнем її захищеності від зовнішнього та внутрішнього впливів. Дані світової і вітчизняної статистики свідчать про тенденцію зростання масштабу комп'ютерних зловживань, що призводять до значних фінансових втрат суб'єктів господарювання різного рівня. Усунення та запобігання інформаційним загрозам різного характеру передбачає побудову чіткої системи діагностики, яка повинна базуватися на оцінці інформаційних ризиків та оцінці зміни економічних, соціальних, техніко-технологічних та інших показників, спричинених зміною стану інформаційної системи підприємства.

Оцінкою інформаційної безпеки займаються з початку появи інформаційних технологій. З цієї тематики є багато праць, але найбільш актуальними та фундаментальними працями є нормативні документи, що зробили вагомий теоретичний та практичний внесок у розв'язання задач забезпечення інформаційної безпеки, а саме: «Помаранчева книга» [1], у якій викладені та систематизовані критерії оцінки захисту комп'ютерних систем; Європейські критерії оцінки безпеки інформаційних технологій [2], що врахували усі недоліки та обмеження, викладені у «Помаранчевій книзі»; Канадські критерії оцінки безпеки надійності комп'ютерних систем [3]; Федеральні критерії США [4], розроблені на замовлення уряду США і спрямовані на усунення обмежень, тощо.

Проте, концептуальні основи оцінки інформаційної безпеки виникли ще в 70-х рр., при формуванні моделі безпеки з повним перекриттям (моделі Клементса-Хоффмана) [14]. У своєму первісному вигляді модель Клементса-Хоффмана була «ідеалізована», проте саме в процесі аналізу даної моделі і виникла проблема необхідності оцінки інформаційних загроз.

Модель побудована виходячи з постулату, що система інформаційної безпеки повинна мати, принаймні, один засіб для забезпечення безпеки на кожному можливому шляху впливу порушника на інформаційну систему. Для опису системи захисту інформації з повним перекриттям розглядаються три підмножини [14]:

множина загроз: $U = \{Ui\}, i = 1, m;$

множина об'єктів захисту $O = \{Oj\}, j = 1, n;$

множина механізмів захисту $M = \{Mk\}, k = 1, r.$

Елементи множин U і O знаходяться між собою у відносинах «загроза – об'єкт». Дуга множина <Ui, Oj> існує тоді, коли Ui – засіб отримання доступу до об'єкта Oj.

Погляди сучасників на проблеми оцінки інформаційної безпеки мають іншу спрямованість на відміну від основоположних концепцій. Відтак, Реверчук Н. Й. пропонує використовувати показники інформаційної безпеки підприємства як продуктивність інформації, коефіцієнт інформаційної озброєності та коефіцієнт захищеності інформації [13]. Такий перелік коефіцієнтів є досить обмеженим. Варто зазначити, що всі три показники відображають лише фінансовий аспект інформаційної безпеки, оскільки в якості вихідних даних для розрахунку зазначених показників виступають витрати на придбання інформаційних ресурсів [7].

На противагу Ілляшенко С. М. рівень інформаційної безпеки визначає часткою неповної, неточної і суперечливої інформації, яка використовується в процесі прийняття управлінських рішень, тобто надає оцінку лише якості інформації, що надається особам, які приймають рішення. Перелік індикаторів потребує доповнення різноманітними показниками,

що характеризують стан програмно-технічної захищеності інформації та інформаційної надійності персоналу [8].

Кравчук О. Я. та Кравчук П. Я. для оцінки рівня інформаційної безпеки пропонують розраховувати п’ять показників, що характеризують рівень інформаційно-аналітичного супроводження діяльності підприємства, захисту комерційної інформації та безпеки документообігу, рівень ділової репутації та іміджу продукції [10].

Шляхом поєднання вищезазначених методичних підходів до оцінки рівня інформаційної безпеки Журавель М.Ю., Полозова Т.В., Стороженко О.В. прпонуєть діагностику рівня інформаційної безпеки підприємства проводити за трьома ключовими напрямками: оцінка програмно-технічної захищеності інформації, оцінка інформаційної надійності персоналу, оцінка інформації, що надається особам, що приймають рішення, інформаційною службою підприємства [7].

Велігура А. В. Пропонує при оцінці використовувати три основні показники. Першим показником служить оцінка небезпек, з якими стикається підприємство. Шляхом оцінки небезпек визначаються загрози для інформації, її вразливість та ймовірність виникнення загроз, а також можливий збиток. Другий показник – це законодавчі, нормативні та договірні вимоги, які повинна дотримуватися організація, її партнери по бізнесу, підрядники та постачальники послуг. Третій показник – це певний набір принципів, цілей і вимог до обробки інформації, розроблених організацією для підтримки своєї діяльності. Визначення вимог до безпеки проводиться шляхом методичної оцінки ризиків. Витрати на підтримку безпеки необхідно збалансувати з шкодою для бізнесу, який може виникнути при порушенні безпеки. Методи оцінки небезпек можуть застосовуватися до всієї організації або лише до її частин, а також до окремих інформаційним системам, системним компонентів і сервісів, в залежності від того, що виявиться найбільш практичним, реалістичним і корисним [6].

Також вона звертає увагу на доцільності методом застосування методу критичних сценаріїв, коли в сценаріях аналізуються ситуації, як уявний злочинець наносить шкоди інформаційній системі підприємства і відповідно знижує здатність підтримувати управління в межах оптимальних параметрів [6].

Залежно від обраного для оцінки інформаційної безпеки критерію Андріанов В. В. розділяє способи оцінки інформаційної безпеки підприємства на оцінку за еталоном, ризик-орієнтовану оцінку та оцінку за економічними показниками. Спосіб оцінки інформаційної безпеки за еталоном зводиться до порівняння діяльності та заходів щодо забезпечення інформаційної безпеки організації з вимогами, закріпленими в еталоні. Тобто проводиться оцінка відповідності системи організації інформаційної безпеки підприємства встановленим еталоном. Під оцінкою відповідності інформаційної безпеки організації встановленим

критеріям розуміється діяльність, пов’язана з прямим або непрямим визначенням виконання або невиконання відповідних вимог інформаційної безпеки в організації. За допомогою оцінки відповідності інформаційної безпеки вимірюється правильність реалізації процесів системи забезпечення інформаційної безпеки організації та ідентифікуються недоліки такої реалізації.

Ризик-орієнтована оцінка інформаційної безпеки організації являє собою спосіб оцінки, при якому розглядаються ризики інформаційної безпеки, що виникають в інформаційній сфері організації, і зіставляються існуючі ризики інформаційної безпеки та вжиті заходи по їх обробці. В результаті повинна бути сформована оцінка здатності організації ефективно управляти ризиками інформаційної безпеки для досягнення своїх цілей.

Спосіб оцінки інформаційної безпеки на основі економічних показників оперує зрозумілими для бізнесу аргументами про необхідність забезпечення та вдосконалення інформаційної безпеки. Для проведення оцінки в якості критеріїв ефективності системи організації інформаційної безпеки використовуються, наприклад, показники сукупної вартості володіння (Total Cost of Ownership – TCO) [5].

Морозова В. І., Врубльовский К. Е. стверджують, що ефективність комплексна система захисту інформації оцінюється як на етапі розробки, так і в процесі експлуатації. В процесі оцінки ефективності комплексної системи захисту інформації, вони виділяють три підходи: класичний, офіційний, експериментальний [12].

Під класичним підходом до оцінки ефективності розуміється використання критеріїв ефективності, значення яких отримуються шляхом моделювання або визначаються за характеристиками реальної інформаційної системи. Такий підхід використовується при розробці і модернізації комплексної системи захисту інформації.

Офіційний підхід передбачає, що політика безпеки інформаційних технологій проводиться державою і повинна спиратися на нормативні акти. Такі документи повинні містити вимоги до захищеності інформації різних категорій конфіденційності важливості. Вимоги можуть задаватися переліком механізмів захисту інформації, які необхідно мати в інформаційній системі, щоб вона відповідала певного класу захисту. Безсумнівною перевагою класифікаторів (стандартів) є їх простота використання. У всіх розвинених країнах розроблені свої стандарти захищеності інформаційних систем. Так, в Міністерстві оборони США використовується стандарт TCSEC, який відомий як Помаранчева книга. Згідно Помаранчевої книги для оцінки інформаційних систем розглядається чотири групи безпеки: A, B, C, D [11].

Під експериментальним підходом розуміється організація процесу визначення ефективності існуючих комплексної системи захисту інформації шляхом спроб подолання захисних механізмів системи фахівцями, які виступають в ролі зловмисників.

Складається план проведення експерименту. У ньому визначаються черговість і матеріально-технічне забезпечення проведення експериментів по визначенню слабких ланок в системі захисту. Служба безпеки до моменту подолання захисту «зловмисниками» повинна ввести в комплексній системі захисту інформації нові механізми захисту або змінити старі, щоб уникнути «злому» системи захисту. Одним з недоліків такого підходу є те, що автор більшість показників розраховує на основі експертного методу, що значно посилює вплив суб'єктивного фактору на кінцевий результат розрахунків. Також запропонована система індикаторів не враховує всіх аспектів інформаційної безпеки підприємства. Зокрема, як і представлена методика не включає показників, що характеризують інформаційну надійність персоналу та програмну захищеність інформації.

Максименко В. Н. та Ясюк Е. В. вирізняють два основні підходи до оцінки інформаційної безпеки підприємства [11].

Перший орієнтується на основні стандарти в сфері інформаційної безпеки або інший набір вимог. Тоді критерій досягнення мети в області безпеки – це виконання заданого набору вимог. Критерій ефективності – мінімальні сумарні витрати на виконання поставлених функціональних вимог. Однак необхідний рівень захищеності в даних документах не завжди строго визначений, тому визначити ефективний рівень захищеності інформаційної системи досить складно.

Другий підхід пов'язаний з оцінкою і управлінням ризиками. Спочатку він визначався відповідно до принципу «розумної достатності» застосованого до сфери забезпечення інформаційної безпеки підприємства. Цей принцип описується набором тверджень:

– абсолютно непереборного захисту досягти неможливо;

– необхідно дотримуватися балансу між витратами на захист та одержуваних ефектом;

– вартість засобів захисту не повинна перевищувати вартості інформації, що захищається;

– витрати порушника на несанкціонований доступ до інформації повинні перевищувати той ефект, який він отримає, здійснивши подібний доступ.

Поряд з найважливішим призначенням оцінки інформаційної безпеки – створення інформаційної потреби для вдосконалення інформаційної безпеки, можливі й інші цілі проведення оцінки інформаційної безпеки такі, як:

– визначення ступеня відповідності встановленим критеріям окремих областей забезпечення інформаційної безпеки, процесів забезпечення інформаційної безпеки, захисних заходів;

– виявлення впливу критичних елементів (факторів) та їх поєднання;

– порівняння зрілості різних процесів забезпечення інформаційної безпеки та порівняння ступеня відповідності різних захисних заходів встановленим вимогам [5, 7, 8, 12].

Таким чином, проведений аналіз дозволив визначити два основних підходи до оцінки інформаційної безпеки підприємства:

перший – на основі характеристик захисних для об'єкта оцінки механізмів і достатності системи захисту. Суть підходу в тому, що висновок про рівень інформаційної безпеки здійснюється на підставі значення показника ефективності системи захисту. При цьому в рамках даного підходу увага приділяється лише одному з аспектів інформаційної безпеки – захист інформації від несанкціонованого доступу.

другий підхід заснований на тісному зв'язку системи показників кількісних оцінок інформаційної безпеки з ефективністю функціонування інформаційної системи в умовах впливу всіх видів загроз інформаційної безпеки. Другий підхід є методологічно більш правильним з точки зору системного аналізу, так як в цьому випадку виконується один з основних принципів системного підходу, який полягає в тому, що кожен елемент системи, виконуючи певну функцію, сприяє досягненню мети (виконання загальносистемної функції).

Узагальнюючи форми, методи та підходи доцільно запропонувати групи показників оцінки інформаційної безпеки, які базується на основних напрямах захисту інформації та враховують: оцінку програмно-технічної захищеності інформації, оцінку витрат на забезпечення інформаційної безпеки, оцінку інформаційної надійності персоналу, оцінку інформації, що надається особам, які приймають рішення, інформаційною службою підприємства, оцінка ризику, надійності, гнучкості та керованості системи захисту інформації (табл. 1).

Таблиця 1

Показники оцінки інформаційної безпеки підприємства [розроблено автором на основі 1-4, 7, 8, 10]

№ п/п	Показники інформаційної безпеки	Характеристика
1	2	3
Оцінка програмно-технічної захищеності інформації		
1	Коефіцієнт фінансування програмної захищеності інформації	Співвідношення вартості програмного забезпечення, яке застосовується для створення інформаційного захисту до загальних витрат на інформаційну безпеку

Продовж. табл. 1

1	2	3
2	Коефіцієнт фінансування технічної захищеності інформації	Співвідношення вартості технічного забезпечення, яке застосовується для створення інформаційного захисту до загальних витрат на інформаційну безпеку
3	Коефіцієнт технічного захисту інформації	Співвідношення кількості відвернутих інформаційних атак до загальної кількості інформаційних атак за певний проміжок часу.
4	Коефіцієнт програмної захищеності інформації	Співвідношення часу безперебійного функціонування корпоративної інформаційної системи до нормативного часу функціонування корпоративної інформаційної системи.
5	Коефіцієнт фінансування програмно-технічної захищеності інформації	Співвідношення витрат на програмно-технічний захист інформаційних ресурсів до витрат на придбання інформаційних ресурсів.
6	Коефіцієнт фінансування інформаційних служб підприємства	Співвідношення витрат утримання інформаційної служби підприємства до загальних витрат підприємства.
7	Коефіцієнт автоматизації програмно-технічної захищеності інформації	Співвідношення автоматизованих процесів спрямованих на програмно-технічний захист інформації до загальної кількості процесів спрямованих на програмно-технічний захист інформації
Оцінка витрат на забезпечення інформаційної безпеки		
8	Коефіцієнт фінансування інформаційної безпеки	Співвідношення витрат на забезпечення інформаційної безпеки підприємства до загальних витрат підприємства.
9	Коефіцієнт фінансування інформаційної безпеки, що забезпечує фінансовий напрям діяльності підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фінансового напряму діяльності підприємства до витрат на забезпечення інформаційної підприємства.
10	Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фізичних об’єктів підприємства до витрат на забезпечення інформаційної підприємства.
11	Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист персоналу підприємства до витрат на забезпечення інформаційної підприємства.
Оцінка інформаційної надійності персоналу		
12	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників, маючих доступ до комерційної таємниці (баз даних, банків даних тощо), що працюють на підприємстві більше одного року до загальної чисельності працівників, що мають доступ до комерційної таємниці (баз даних, банків даних тощо).
13	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників, звільнених за причиною витоку інформації до загальної чисельності звільнених працівників.
14	Коефіцієнт підготовленості персоналу до розпізнавання загроз інформаційній безпеці	Співвідношення чисельності, ненавмисні дії яких призвели до витоку інформації через низький рівень компетентності персоналу та невміння розпізнавання загроз інформаційній безпеці до загальної чисельності працівників, що мають доступ до закритої інформації.
15	Коефіцієнт правової захищеності інформації	Співвідношення обсягу інформації, розголошення якої може спричинити негативні наслідки для підприємства до загального обсягу юридично захищеної інформації.

Продовж. табл. 1

1	2	3
16	Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	Співвідношення інформаційних загроз (інформаційних атак), які відвернуті через дії персоналу, який забезпечує інформаційну безпеку до загальної кількості інформаційних атак за певний проміжок часу.
Оцінка інформації, що надається особам, які приймають рішення, інформаційною службою підприємства		
17	Коефіцієнт повноти інформації	Співвідношення обсягу інформації, що є в розпорядженні ОПР до обсягу інформації, необхідної для ухвалення обґрунтованого рішення.
18	Коефіцієнт точності інформації	Співвідношення обсягу релевантної інформації до загального обсягу наявної в розпорядженні ОПР інформації.
19	Коефіцієнт суперечливості інформації	Співвідношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації.
20	Коефіцієнт своєчасності надання інформації	Співвідношення обсягу своєчасно наданої ОПР інформації до обсягу інформації, необхідної для ухвалення обґрунтованого рішення.
21	Коефіцієнт надійності інформації	Співвідношення обсягу інформації, наданої ОПР з перевірених джерел до загального обсягу наданої ОПР інформації.
Оцінка системи захисту інформації		
22	Ступінь інформаційного ризику	відсоток втрат (у грошову вираженні) спричинених пошкодженням інформаційної цілісності підприємства
23	Гнучкість системи інформаційної безпеки підприємства	Здатність системи управління інформаційною безпекою швидко адаптувати організаційну побудову до зовнішніх та внутрішніх потреб.
24	Коефіцієнт керованості системи інформаційної безпеки підприємства	Співвідношення компетентостей керівного персоналу системи інформаційної безпеки до загальних компетентностей, якими повинен володіти керівник відповідного рівня.
25	Частка програмного забезпечення, розробленого працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства.	
26	Частка технічних засобів, розроблених працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства.	

Висновки та перспективи подальших досліджень.

Особливістю пропонованої системи показників оцінки інформаційної безпеки підприємства є те, що вона охоплює економічні показники, технічні та програмні параметри системи інформаційної безпеки та надає оцінку персоналу, який здійснює управління зазначеною підсистемою. Також така система показників оцінки інформаційної безпеки підприємства може бути застосована на будь-кому підприємстві, не залежно від його розміру, сфери та напряму діяльності, що робить її універсальною. Водночас, варто зазначити, що в залежності від мети діагностики рівня інформаційної безпеки показники в кожній групі можуть бути доповнені або замінені.

Важливою проблемою залишається взаємоузгодженість пропонованих показників в межах групи та між собою, а також розробка інтегрального показника інформаційної безпеки підприємства, що і є перспективним напрямом подальших досліджень.

Список використаної літератури:

1. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1985 [Electronic resource]. – Access mode : http://csrc.nist.gov/publications/history/dod85.pdf

2. Information Tecnhology Security Evaluation Criteria, v. 1.2. – Office for Official ublications of the European Communities, Printed and published by the Department of Trade and Industry, London, 1991. – 164 p.

3. Канадські критерії безпеки комп'ютерних систем (Canadian Trusted Computer Product Evaluation Criteria. – [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/3506169_The_Canadian_Trusted_Computer_Product_Evaluation_Criteria_CTCPEC

4. Федеральні критерії безпеки інформаційних технологій» (Federal Criteria for Information Technology Security. – [Електронний ресурс]. – Режим доступу: https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf

5. Андрианов В. В. Оценка информационной безопасности бизнеса / В. В. Андрианов, В. Б. Голованов, Н. А. Голдуев, С. Л. Зефиров. – 2-е изд., перераб. и доп. – М.: ЦИПСиР: Альпина Паблишерз, 2011. – 373 с. + 8 с. вкл.

6. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства / А. В. Велігура // Управління проектами та розвиток виробництва. – 2014. – №4(52). – С. 28-39.

7. Журавель М. Ю. Формування системи показників оцінки рівня інформаційної безпеки підприємства / Журавель М. Ю., Полозова Т. В., Стороженко О. В. // Вісник економіки транспорту і промисловості. – 2011. – № 33. – С. 171-177.

8. Ілляшенко С.М. Економічний ризик [Текст]: навч. посіб. 2-ге вид., доп., перероб. / С.М. Ілляшенко – К.: Центр навчальної літератури, 2004. – 220 с.

9. Кононова В. О. Оцінка засобів захисту інформаційних ресурсів / Кононова В. О., Харкянен О. В., Грибков С. В. // Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі. – 2014. – № 806. – С. 99-105. – Режим доступу: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_18

10. Кравчук О. Я. Діагностика рівня та критерії оцінки корпоративної безпеки суб'єктів господарювання / О. Я. Кравчук, П. Я. Кравчук // Економічні науки. Серія «Економіка та менеджмент»: збірник наукових праць. Луцький державний технічний університет. – Випуск 1. Редкол.: відп. ред. д.е.н., проф. Герасимчук З. В. – Луцьк, 2004. – С. 85-109.

11. Максименко В. Н. Основные подходы к анализу и оценке рисков информационной безопасности / В. Н. Максименко, Е. В. Ясюк // Экономика и качество систем святи. – 2017. – 2/2017. – С. 42-48.

12. Морозова В. И., Врублевский К. Э. Защита информации в вычислительных системах: [учеб. пособ.] / Под ред. В.И.Морозовой – М.: МИИТ, 2008 – 122 с.

13. Реверчук Н.Й. Управління економічною безпекою підприємницьких структур: [монограф.] / Н.Й. Реверчук. – Львів: ЛБІ НБУ, 2004. – 195 с.

14. Хоффман Л. Дж. Современные методы защиты информации // Пер. с англ. – М.: Советское радио, 1980. – 264 с.

Дячков Д. В. Методические подходы к оценке информационной безопасности предприятия

В статье определена актуальность исследования методических подходов к оценке информационной безопасности предприятия. Важность этого направления исследования заключается, прежде всего, в обосновании необходимости формирования комплексной системы диагностики уровня информационной безопасности, количественной и качественной оценки состояния уровня информационной защищенности предприятия.

Проведенный анализ позволил определить два основных подхода к оценке информационной безопасности предприятия: первый основан на характеристике защитных для объекта оценки механизмов и достаточности системы защиты; второй подход основан на тесной связи системы показателей количественных оценок информационной безопасности с эффективностью функционирования информационной системы в условиях воздействия всех видов угроз информационной безопасности.

На основе обобщения форм, методов и подходов предложена система показателей оценки информационной безопасности, основанная на базовых направлениях защиты информации, что учитывают: оценку программно-технической защищенности информации, оценку затрат на обеспечение информационной безопасности, оценку информационной надежности персонала, оценку информации, предоставляемой лицам, которые принимают решения, информационной службой предприятия, оценку риска, надежности, гибкости и управляемости системы защиты информации.

Ключевые слова: *информационная безопасность, методический подход, оценка информационной безопасности, показатели, программно-техническая защита, угрозы, управление системой информационной безопасности.*

Diachkov D. V. Methodical approaches to assessment of information security of enterprise

The article defines the relevance study of methodological approaches to assessing the information security of enterprise. The importance of this research area is, first of all, in justifying the need to form a comprehensive system for diagnosing the level of information security, quantitative and qualitative assessment of the state of the information security level of the enterprise.

The analysis made it possible to identify two basic approaches to assessing the information security of an enterprise: the first is based on the characteristics of the protective mechanisms for the object and the adequacy of the protection system; the second approach is based on the close connection of the system of indicators of quantitative assessments of information security with the effectiveness of the information system in the impact of all types of threats to information security.

Based on the generalization of forms, methods and approaches, a system of indicators for assessing information security based on the basic directions of information protection is proposed, which takes into account: the evaluation of software and information security, the assessment of information security costs, the assessment of information reliability of personnel, the evaluation of information provided to individuals, which make decisions, information service of the enterprise, risk assessment, reliability, flexibility and controllability of the information security system.

Keywords: indicators, information security assessment, information security management, information security, methodical approach, software and hardware protection, threats.