Отже, згідно розрахунків наведених у табл. 2, рівень фінансової безпеки повинен наближатися до одиниці. Чим вище значення, тим вищій рівень захищеності має підприємство.

Література

1. Антонова О. Систематизация методических подходов до оцінки фінансової безпеки підприємтсва / О. Антонова // Економіки . – 2010. – №6 (106). – С. 3-7.

2 Гришко Н.Є. Методичні аспекти оцінки фінансової складової економічної безпеки підприємства / Н.Є. Гришко // Регіональні перспективи. – 2002. – № 1 – С. 112-115.

3 Молодецька О.М. Комплексна оцінка економічної безпеки підприємтва (на прикладі гірничих підприємств): автореф. дис. канд. екон. наук: 08.00.04. – Кривий Ріг, 2010. – 22 с.

4. Мунтіян В.І. Економічна безпека України / В.І. Муниіян. – К.: Вид-во КВІЦ, 1999. – 216 с.

5. Папехин Р.С. Факторы финансовой устойчивости и безопасности предприятия: автореф. дис. канд. эконом. наук. – Волгоград., 2007. – 21 с.

338.486.2

Танцюра М.Ю., старший викладач,
Кримський економічний інститут ДВНЗ «КНЕУ імені В. Гетьмана»

ОРГАНІЗАЦІЙНЕ ТА РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТУРИСТИЧНИХ ПІДПРИЄМСТВ

Виходячи з результатів аналізу інформаційних загроз та засобів інформаційного захисту туристичних підприємств [1, 2], встановлено їх суттєву невідповідність, яка приводить до неефективності системи інформаційної безпеки туристичних підприємств. У зв'язку з цим, виникає необхідність у визначенні заходів, які б дозволили забезпечити ефективність системи інформаційної безпеки туристичних підприємств.

Останнім часом проблемам інформаційного забезпечення діяльності туристичних підприємств приділяється все більше уваги з боку вітчизняних вчених. Никитин Л.Н. визначив закономірності інформаційного забезпечення та їх використання у туристичному бізнесі [3]. Дітковська М.Ю. обгрунтувала формування інформаційного забезпечення туристичної галузі на регіональному рівні [4]. Мельниченко С.В. дослідив інформаційні технології в управлінні суб'єктами туристичної діяльності [5].

У той же час, невирішеними залишаються питання організаційного та ресурсного забезпечення ефективності системи інформаційної безпеки туристичних підприємств.

Мета статті: визначити зміст організаційного та ресурсного забезпечення ефективності системи інформаційної безпеки туристичних підприємств.

Більшість вчених-економістів згодні, що ефективність – це відношення отриманого результату до здійснених витрат для його досягнення [6, 7, 8]. Отже, у застосуванні до системи інформаційної безпеки туристичного підприємства, ефективність – це співвідношення приросту рівня інформаційної безпеки до приросту витрат ресурсів на формування та функціонування системи інформаційної безпеки.

Виходячи з наданого визначення ефективності, існує два основних напрямки її забезпечення:

1) підвищення рівня інформаційної безпеки туристичного підприємства;

2) скорочення витрат ресурсів на формування та функціонування системи інформаційної безпеки.

Перший напрямок забезпечення ефективності ми пропонуємо реалізувати за допомогою комплексу організаційного забезпечення ефективності системи інформаційної безпеки туристичних підприємств, який включає наступні заходи: підвищення рівня організації системи інформаційної безпеки туристичного підприємства на основі її комплексної регламентації; розробка ефективної системи навчання та тестування персоналу туристичного підприємства на основі компетентнісного підходу; реалізація заходів з матеріального стимулювання персоналу туристичного підприємства до виконання правил інформаційної безпеки; запровадження пріоритетних форм функціонування системи інформаційної безпеки туристичного підприємства (математизації, автоматизації, інтелектуалізації та інноватизації).

Комплексна регламентація системи інформаційної безпеки підприємства передбачає розробку набору інструктивних документів з організації інформаційного захисту, які повинні затверджуватися

наказом керівництва туристичного підприємства та регулювати наступні питання: визначення основних термінів з інформаційної безпеки; структура та функції підрозділу інформаційної безпеки підприємства; права та обов'язки персоналу у сфері інформаційного захисту; відповідальність за порушення правил інформаційного захисту; регламентація режиму інформаційного захисту; встановлення профілів інформаційного захисту; порядок управління доступом; порядок управління інцидентами; порядок зовнішніх інформаційних зносин.

Іншим важливим питанням організаційного характеру є визначення необхідності створення підпрозділу інформаційної безпеки підприємства (служби інформаційної безпеки) та її кадрового, матеріально-технічного та фінансового забезпечення. Відповідь на це питання потребує диференційованого підходу, оскільки кожне туристичне підприємство незважаючи на загальну галузеву належність має особливі риси (табл. 1).

Для запровадження системи навчання та контролю персоналу необхідно, перш за все, визначити питання, які підлягають вивченню, орієнтуючись на вимоги наказу з інформаційної політики та статистики інцидентів. Крім того, важливими питаннями є періодичність та форми навчання, які визначають виходячи з розмірів підприємства.

Таблиця 1

Фактори формування служби інформаційної безпеки (СІБ)

Розмір підприємства	Відношення інформаційних збитків до власного капіталу		
	>0,6	≈ 0,5	<0,2
Велике	Багатопрофільна внутрішня СІБ з розширеними повноваженями та залучення зовнішніх спеціалістів	Багатопрофільна внутрішня СІБ з розширеними повноваженями	Багатопрофільна внутрішня СІБ
Середнє	Штатний співробітник з повноваженіми СІБ та зовнішні спеціалісти	Штатний співробітник з повноваженіми СІБ	Сумісник з повноваженнями СІБ
Мале	Сумісник з повноваженнями СІБ та зовнішні спеціалісти	Зовнішні спеціалісти з питань інформаційної безпеки	Керівник малого підприємства та непрофільні спеціалісти

При розробці програми навчання особливу увагу слід приділити тим питанням інформаційної безпеки, які пов'язані з виникненням на підприємстві найбільших збитків та шкоди. Також, слід врахувати перспективні напрямки розвитку підприємства та зміни зовнішнього середовища підприємства, які можуть призвести до суттєвої зміни стратегічних пріоритетів та вимог до системи інформаційної безпеки підприємства.

Обов'язковим елементом системи навчання та контролю персоналу, ми вважаємо, є не тільки контроль знань, вмінь та навичок співробітників, але й контроль у процесі виконання службових обов'язків. Результати такого контролю необхідно використовувати для двох основних функцій [9, 10, 11]:

1) виявлення порушень та винних у їх скоєнні для притягнення їх до відповідальності;

2) виявлення співробітників, які сумлінно виконують правила інформаційної безпеки та їх заохочення.

Тобто, контроль персоналу повинен виконувати не лише каральну функцію, але й стимулюючу, що дозволить використовувати переваги позитивної мотивації.

Ефективність матеріального стимулювання співробітників, які сумлінно виконують правила інформаційної безпеки (ПІБ) обумовлена наступними причинами:

більшість інцидентів інформаційної безпеки трапляється з вини людського фактору;

майже усі інформаційні процеси на підприємстві здійснюються за участю персоналу;

основним джерелом доходів більшості українців є зарплата, а її середній по країні розмір не відповідає вимогам нормального існування.

Методика розподілу фонду преміювання персоналу підприємства за сумлінне виконання правил інформаційної безпеки (ФПБ) включає декілька етапів:

1) визначення загального розміру відповідного фонду преміювання;

2) вибір критеріїв преміювання з відповідного фонду;

3) встановлення пріоритетності критеріїв преміювання;

4) регламентація порядку оцінювання за кожним критерієм;

5) відбір суб'єктів, що здійснюватимуть оцінку;

6) розрахунок інтегральної оцінки кожного співробітника за обраними критеріями з врахуванням їх пріоритету;

7) розподіл відповідного фонду преміювання з врахуванням інтегральної оцінки співробітників;

8) апостеріорна оцінка ефективності преміювання.

Другим напрямком забезпечення ефективності системи інформаційної безпеки туристичних підприємств, як було визначено вище, є скорочення витрат ресурсів на формування та функціонування системи інформаційної безпеки. Для реалізації цього напрямку ми пропонуємо оптимізувати структуру ресурсозабезпечення системи інформаційної безпеки туристичного підприємства з метою максимізації синергетичного ефекту [12, 13, 14] у формі зниження витрат ресурсів.

Структуру ресурсозабезпечення відобразимо за допомогою ресурсної матриці туристичного підприємства (табл. 2).

Як видно з табл. 2, ресурсна матриця системи інформаційної безпеки туристичного підприємства включає наступні елементи: $C = \{c_i\}$ – множина ресурсів; $S = \{s_j\}$ – множина джерел ресурсів; $P = \{p_{ij}\}$ – вартість ресурсів і-го виду із j-го джерела ресурсів; $R = \{r_{ij}\}$ – обсяг ресурсів і-го виду, отриманих із j-го джерела ресурсів; $TP = \sum p_{ij} r_{ij}$ – загальна вартість ресурсів.

Таблиця 2

Ресурсна матриця системи інформаційної безпеки туристичного підприємства

Ресурсні потреби	Джерела ресурсів				
	S_1	S_2	S_3	...	S_j
C_1	p_{11} r_{11}	p_{12} r_{12}	p_{13} r_{13}	…	p_{1j} r_{1j}
...	...	...	...	...	...
C_i	p_{i1} r_{i1}	p_{i2} r_{i2}	p_{i3} r_{i3}	…	p_{ij} r_{ij}

Таким чином, для оптимізації за допомогою ресурсної матриці доцільно скористатися методами математичного програмування, що дозволит знайти таку структуру ресурсозабезпечення, яка забезпечить мінімум витрат при заданому рівні задоволення ресурсних потреб туристичного підприємства.

Реалізація розглянутих пропозицій щодо організаційного та ресурсного забезпечення системи інформаційної безпеки туристичних підприємств дозволить підвищити рівень інформаційної безпеки та знизити витрати на формування та функціонування системи інформаційної безпеки туристичних підприємств. У подальших дослідженнях проблеми забезпечення ефективності системи інформаційної безпеки туристичних підприємств необхідно обгрунтувати визначення пріоритетів реалізації внутрішньо- господарських заходів з забезпечення ефективності відповідної системи.

Література

1. Танцюра М.Ю. Аналіз інформаційних загроз туристичних підприємств АРК / М.Ю. Танцюра // Вісник Тернопільського національного економічного університету. – 2011. – № 2. – С. 81-87.

2. Танцюра М.Ю. Економічний аналіз рівня інформаційного захисту під-приємства / М.Ю. Танцюра // Економіка промисловості. – 2011. – № 1. – С.203-206.

3. Никитин Л. Н. Закономерности информационного обеспечения и их использования в туристическом бизнесе / Л. Н. Никитин, Т. В. Никитина // Вісник ДІТБ. Сер. «Підприємництво, менеджмент та маркетинг в туристичній сфері». – 2000. – № 4. – С.146-152.

4. Дітковська М.Ю. Формування інформаційного забезпечення туристичної галузі на регіональному рівні // Вісник Чернігівського державного технологічного університету. Серія «Економічні науки». – 2011. – № 3(52). – С. 353-357.

5. Мельниченко С.В. Інформаційні технології в управлінні суб'єктами туристичної діяльності: автореф. дис... д-ра екон. наук: 08.00.04 / С.В. Мельниченко; Київ. нац. торг.-екон. ун-т. – К., 2008. – 46 с.

6. Современный экономический словарь / Б.А. Райзберг, Л.Ш. Лозовский, Е.Б. Стародубцева. – М.: ИНФРА-М, 2006. – 495 с.

7. Большой экономический словарь: 26500 терминов / авт. и сост. А.Н. Азрилиян, О.М. Азрилиян., Е.В. Калашникова, О.В. Квардакова. – М.: Ин-т новой экономики, 2007. – 1472с.

8. Новиков В.А. Толковый словарь по рыночной экономике / В.А. Новиков. – М.: Экономистъ, 2007. – 384с.

9. Стернійчук М.А. Сутність, складові та мотивація до професійного навчання персоналу підприємства / М.А. Стернійчук, О.В. Захарова // Проблемы управления производственно-экономической деятельностью

субъектов хозяйствования: материалы III Всеукр. научн. конф. студ., 23 апреля 2009 г., г. Донецк, ДонНТУ. – Т.1. – Донецк: СПД Воробьев, 2009. – С.8-11.

10. Адаменко Е. Профессиональное обучение персонала / Е. Адаменко // Менеджер по персоналу. – 2006. – № 11. – С. 58-62

11. Дрозач М. Підготовка робітничих кадрів на виробництві через мережу професійно-технічних навчальних закладів / М. Дроздач // Україна: аспекти праці. – 2006. – № 7. – С. 36-41.

12. Баранников В.В. Синтез комбинированных имитационно-оптимизационных моделей кругооборота оборотных активов (синергетический эффект) / В.В. Баранников // Вісник Донецького національного університету. – Сер. В: «Економіка і право». – 2008. – Вип.2. – С. 347-350.

13. Бычкова Г.М. Обоснование применения синергетического подхода к оценке эффективности функционирования кластера / Г.М. Бычкова // Известия Иркутской государственной экономической академии. – 2008. – № 6 (62). – С.66-68.

14. Ханова А.А. Синергетический эффект управления организацией на основе сбалансированной системы показателей / А.А. Ханова // Прикаспийский журнал: управление и высокие технологии. – 2010. – № 4 (12). – С.36-40.

Рецензент докт. екон. наук, професор С.П. Наливайченко

338.48:005.922.1:33

Кокорєва О.В., старший викладач,
Херсонський національний технічний університет

ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ТУРИСТИЧНИХ ПІДПРИЄМСТВ НА ОСНОВІ МАТРИЦІ «ЕКОНОМІЧНА БЕЗПЕКА ТУРИСТИЧНИХ ПІДПРИЄМСТВ – РИЗИК»

Світова економічна криза, вади законодавства, економічні реформи уряду, некомпетентність персоналу, тиск збоку кримінальних угруповань – все це залишає свій відбиток на діяльності підприємств України. Успішне функціонування та економічний розвиток туристичних фірм багато в чому залежить від ефективних управлінських рішень щодо забезпечення їх економічної безпеки, яка значною мірою визначається надійністю системи захисту від внутрішніх ризиків і зовнішніх загроз. Тому проблема пошуку і впровадження в практику нових форм і методів управління економічною безпекою туристичних підприємств є важливою, вирішення якої дозволить підготувати і реалізувати відповідні заходи і розробити оптимальні стратегії дій.

Проблеми, що пов'язані з управлінням економічної безпеки у сфері туризму, висвітлені у працях відомих фахівців: Козаченко Г.В., Ляшенко О.М., Олексюк О.І., Савіної Г.Г., Ткач В.О., Цьохли С.Ю., Шульгіної Л.М.

Проведений аналіз літературних джерел та публікацій за даною проблематикою дозволили зробити висновок про те, що питання вдосконалення управління економічною безпекою туристичних підприємств є недостатньо розробленими як на науковому так і в практичному аспектах.

Метою статті є розробка матриці «Економічна безпека туристичних підприємств – Ризик», що дозволить поєднати різні кластери інформації та наочно визначити зону ризику з метою прискорення прийняття ефективних управлінських рішень.

Інтегральний показник економічної безпеки туристичного підприємства свідчить про рівень його захищеності від ризиків і загроз. Для прискорення прийняття ефективних управлінських рішень нами пропонується використання матриці «Економічна безпека туристичного підприємства – Ризик», що базується на розподілі туристичних підприємств за зонами ризику (на основі діапазонів ймовірності ризику за Чебишевим В.І.), і діапазонів відстані до еталонної точки інтегрального показника економічної безпеки туристичних підприємств ($I_{ЕБТП}$).

Вертикаль мартиці формують діапазони ймовірностей ризиків, визначені Чебишевим В.І.:

Діапазон мінімального ризику – характеризується рівнем ризику від 0,0 до 0,1;

Діапазон невисокого ризику – характеризується рівнем ризику від 0,1 до 0,3;

Діапазон середнього ризику – характеризується рівнем ризику від 0,3 до 0,4;

Діапазон високого ризику – характеризується рівнем ризику від 0,4 до 0,6;

Діапазон максимального ризику – характеризується рівнем ризику від 0,6 до 0,8;

Діапазон критичного ризику – характеризується рівнем ризику від 0,8 до 1,0.

Горизонталь матриці формують значення інтегрального показника економічної безпеки туристичних підприємств ($I_{ЕБТП}$) за наведеними нижче діапазонами: