секторов экономики, развитию благоприятного инвестиционного климата и инфраструктуры, созданию новых производств и развитию человеческого капитала позволит реализовать в регионе президентскую стратегию модернизации страны.

Список литературы

1. О развитии малого и среднего предпринимательства в Российской Федерации: [Федеральный закон Российской Федерации от 24 июля 2007 г.– № 209-ФЗ].

2. Об инновационной деятельности и инновационной политике на территории Белгородской области: [закон Белгородской области от 01 октября 2009 года № 296] [Электронный ресурс]. – Режим доступа : <http://www.innovbusiness.ru/>.

3. Информация об экономическом развитии Белгородской области в январе-марте 2011 года [Электронный ресурс]. – Режим доступа : <www.belregion.ru/region/economy/>.

4. Институт Инноваций Инфраструктуры и Инвестиций – Центр развития карьеры НИУ ВШЭ [Электронный ресурс]. – Режим доступа : <http://five-i.ru/>.

5. Белгородская область вошла в тридцатку лучших регионов для бизнеса по версии Forbes [Электронный ресурс]. – Режим доступа : <http://www.bel.ru/news/business/2011/05/30/55070.html>.

6. Информационный портал поддержки малого и среднего бизнеса белгородской области [Электронный ресурс] [2011]. – Режим доступа : <http://www.mb31.ru/>.

МЕТОДИЧНІ ЗАСАДИ ОЦІНКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

А.С. Крутова, д-р екон. наук, ХДУХТ
А.В. Янчев, канд. екон. наук, ХДУХТ

Господарський кодекс України наполягає на віднесенні інформації до складу ресурсів організації, поряд із матеріально-технічними, фінансовими, трудовими, природними й іншими. Тому одним із найважливіших завдань сучасного бухгалтерського обліку є запровадження дієвих заходів інформаційної безпеки та контроль за збереженням такого важливого для підприємства виду активів як інформаційні ресурси.

Згідно зі ст. 1 Закону України «Про основи національної безпеки України» безпека визначається, як захищеність життєво важливих інтересів людини і громадянина, суспільства й держави, за якої забезпечуються сталий розвиток суспільства, своєчасне

виявлення, запобігання й нейтралізація реальних і потенційних загроз національним інтересам. Не завжди під поняттям «захист інтересів» малася на увазі також безпека інформаційна. Однак за сучасних умов інформаційна сфера розглядається як системоутворюючий чинник життя суспільства, що активно впливає на стан політичної, економічної, оборонної й інших складових безпеки України. Інформатизація, яка є визначальним чинником впливу на розвиток суспільно-економічної формації, зумовлює істотну залежність національної безпеки України від інформаційної, і в ході подальшого технічного прогресу така залежність неухильно зростатиме.

Сьогодні проблеми інформаційної безпеки непокоять практично всіх: силові структури, органи влади, юридичних і фізичних осіб. Особливої актуальності функції інформаційного захисту набувають для суб'єктів господарювання, які, окрім інформації суто економічного характеру, що становить комерційну таємницю підприємства, зберігають у своїх базах персональні дані високого ступеня секретності, наприклад, платіжні реквізити своїх покупців. Несанкціоноване одержання такої інформації є найбільш спокусливим для потенційних порушників інформаційної безпеки господарюючого суб'єкта. Законом «Про захист персональних даних» запроваджено, що використання персональних даних власником бази здійснюється у разі створення ним умов для захисту цих даних, тобто створення безпечних умов збирання, зберігання й обробки такої секретної інформації покладається на власника бази даних – суб'єкта господарювання і є однією з умов його функціонування.

Розв'язання питання про розробку на підприємстві ефективної політики інформаційної безпеки пов'язане з проблемою вибору критеріїв і показників захищеності, а також запроваджених прийнятих механізмів й ефективності системи інформаційної безпеки. Тому до функцій контролю за схоронністю активів підприємства необхідно додати завдання контролю схоронності такого виду активів, як інформаційні ресурси. Для цього необхідно розробити систему розрахунку рівня збитку унаслідок можливого інциденту порушення інформаційної безпеки – інтегрованого якісного показника, який комплексно характеризує можливі фінансові збитки, втрату репутації, ймовірність настання цивільної відповідальності та ін.

Ризик інформаційної безпеки слід трактувати як функцію (fR) від трьох параметрів: ймовірності загроз захисту системи (threats – T), ступеня вразливості системи (vulnerability – V) та оцінки можливого збитку від порушення безпеки (loss – L):

$$fR = \sum_{t=1} Rt\,, \qquad (1)$$

де t – існуючі види загроз, а Rt – ймовірність настання інциденту і-го виду загроз.

Загальний рівень ризику для бізнес-процесів підприємства, продуктів, персоналу, фізичного середовища тощо дорівнює максимальній величині з усіх ризиків за кожною парою загроза/вразливість. Означений інтегрований показник ризику настання інциденту інформаційної безпеки має визначатися за схемою (рис.):

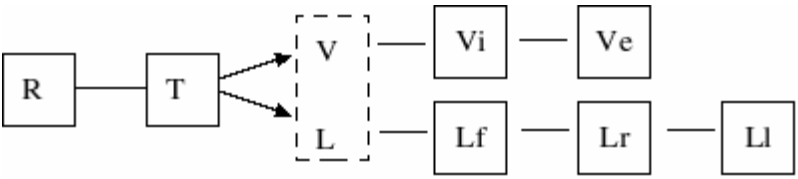

Рисунок – Схема формування інтегрованого показника інформаційного ризику (R – ризик інформаційної безпеки; T – ризик загроз; V – ризики вразливості системи: Vi – внутрішні; Ve – зовнішні; L – ризик збитків: Lf – фінансових; Lr – репутації; Ll – правових)

Рівень ризику настання певного виду загроз (природних, техногенних, навмисних і ненавмисних людських) залежить, по-перше, від ступеня вразливості системи, що характеризується мірою несанкціонованої доступності інформаційних ресурсів, які підлягають захисту як зовні, так і всередині підприємства. По-друге, рівень ризику є пропорційним збиткам, які можуть спричинити втрату рівня фінансового стану або репутації підприємства. При цьому кожний із зазначених параметрів необхідно розглядати в рамках математичної ймовірнісної моделі, побудованої на базі експертних оцінок, за наявності достатньої статистичної бази, що ведеться на рівні: а) держави; б) громадських і консультаційних організацій, в) підприємства. Дані таких обстежень мають оприлюднюватися на порталах органів державної влади та сайтах громадських організацій, що сприятиме підвищенню рівня обізнаності користувачів й зміцненню довіри до електронної економічної діяльності. Для визначення показників пропонуємо скористатися шкалою вірогідності настання інциденту інформаційної безпеки (табл. 1), завданої шкоди від настанні інциденту порушення безпеки (табл. 2) та загального рівня інформаційного ризику (табл. 3) [ISO 27002].

Таблиця 1 – **Шкала оцінки вірогідності настання інциденту інформаційної безпеки**

Вірогідність інциденту	**Частота**	**Рейтинг**
Незначна	Не зафіксовано	0
Дуже низька	2 – 3 рази за 5 років	1
Низька	Один раз на рік	2
Середня	Раз на шість місяців	3
Висока	Рідше одного разу на місяць	4
Дуже висока	Частіше одного разу на місяць	5
Екстремальна	Раз на день	6

Таблиця 2 – **Шкала оцінки шкоди від настання інциденту інформаційної безпеки**

Розмір завданої шкоди	**Рівень шкоди**	**Рейтинг**
Незначний	Мінімальний або невідчутний вплив	0
Мінімальний	Не вимагає додаткових зусиль на запобігання шкідливому впливу	1
Суттєвий	Відчутна шкода, що потребує додаткових дій на запобігання	2
Шкідливий	Потребує суттєвих витрат ресурсів Призводить до втрати репутації або конфіденційності	3
Серйозний	Тривалі простої та пошкодження засобів комунікації Компрометація значних масивів даних та послуг	4
Тяжкий	Перманентна відмова системи Повна компрометація даних	5

Таблиця 3 – **Шкала оцінки ризику інформаційної безпеки**

Рейтинг	**0**	**1 – 3**	**4 – 7**	**8 – 14**	**15 – 19**	**20 – 30**
Рівень ризику	Відсутній	Низький	Середній	Високий	Критичний	Екстремальний

При цьому формується масив оцінок респондентів – $m[i, j]$ (де: i – загальна кількість показників) стосовно досліджуваного суб'єкта здійснення електронної торгівлі. Після чого необхідно розрахувати середнє значення за кожним показником (2) та комплексний показник рівня інформаційної безпеки (3).

$$\overline{m_i} = \frac{\sum_{j=1}^{R} m[i, j]}{R}, \tag{2}$$

де R – загальна кількість респондентів.

$$y = \frac{\sum_{i=1}^{Q} \overline{m_i} \times \alpha_i}{R}, \tag{3}$$

де Q – загальна кількість показників інформаційної безпеки.

Важливе місце в забезпеченні інформаційного захисту необхідно відводити використанню засобів зовнішнього контролю. Такі функції можуть взяти на себе спеціалізовані відділи з контролю інформаційних технологій (IT-аудитори). Запровадження незалежної аудиторської перевірки стандартів, процедур і практики інформаційного захисту сприятиме підвищенню рівня захищеності інформаційних ресурсів від утрати, ушкодження або нецільового використання.

Узагальнюючи вищесказане, необхідно відзначити, що інформаційна безпека електронної торгівлі характеризується ступенем її захищеності і, отже, стійкістю основних бізнес-процесів та інформаційних ресурсів до небезпечних, деструктивних, дестабілізуючих інформаційних дій. Інформаційна безпека визначається здатністю нейтралізувати такі дії. Розробка механізмів забезпечення інформаційної безпеки комерційної діяльності в Україні тісно пов'язана із заходами щодо інформатизації суспільства взагалі. За цих умов право повинно стати на захист глобальних цінностей. І це насамперед стосується добробуту людини й умов функціонування та розвитку суб'єктів підприємницької діяльності. Інформаційну систему

не можна регулювати тільки виходячи з інтересів розвитку технологій та інформаційних ресурсів. Охоплюючи всі сфери діяльності, інформатизація кидає нові виклики інформаційній безпеці і створює для неї нові загрози. Поодинці комерційні підприємства не зможуть створити ефективну систему інформаційного захисту. Настала нагальна потреба у державному контролі та регулюванні правового режиму інформаційної безпеки, в основу якого має бути покладений принцип пріоритету людини, особистості, суспільства. Це дозволить забезпечити схоронність інформаційних ресурсів підприємства та сприятиме зміцненню довіри до електронної економічної діяльності.

СИСТЕМНЫЙ ПОДХОД В ФИНАНСОВОМ УПРАВЛЕНИИ ЧЕЛОВЕЧЕСКИМ КАПИТАЛОМ

В.В. Богатырева, канд. экон. наук,
УО «ПГУ», Новополоцк, Республика Беларусь

Финансовые решения базируются на общих методологических основах их принятия, т.е. на применении основных подходов. Одним из важнейших подходов, сущность которого позволяет определить место человеческого капитала в управляемой и управляющей подсистемах открытой системы управления, функционирующей в сложившейся среде определенной организации и активно взаимодействующей с внешней средой, является системный подход финансового менеджмента.

В финансовом управлении системный подход начал применяться в середине XX столетия. Основными учеными, выделявшими его, были исследователи Л. фон Берталанфи, А.А. Богданов, Г. Саймон, П. Друкер, А. Чандлер. Основоположник теории систем Людвиг фон Берталанфи определял систему как комплекс взаимодействующих элементов или как совокупность элементов, находящихся в определенных отношениях друг с другом и со средой [1]. Рассматривают систему и, соответственно, системный подход в управлении как некую целостность взаимосвязанных элементов с определенными признаками и другие ученые. Так, А. Холл определяет систему как множество предметов вместе со связями между предметами и между их признаками [2]. По определению Р. Акоффа «системный подход в управлении основывается на том, что всякая организация представляет собой систему, состоящую из частей, каждая из которых обладает своими собственными целями» [3]. При описании сущности современных