

моделі; впровадження мережевої моделі підприємництва в діяльність підприємств побутового обслуговування.

Література

1. Ігнат'єва І.А., Кузьмич О.Г. Моніторинг як інформаційна основа для формування управлінських рішень щодо розвитку підприємств побутового обслуговування // Економіка та держава. – Київ, 2009. - № 10. – С.20-22.
2. Савіна Г.Г. Розроблення системи управління розвитком трудового потенціалу регіонів України в контексті світових інтеграційних процесів // Монографія - Херсон: ХНТУ, 2010.
3. Христофорова І.В. Коровин Е.М., Бушуєва Л.И. Опыт изучения потребностей населения в бытовых услугах // «Маркетинг» - 1998. - № 4.- С. 28-36.
4. Бушуєва Л.И., Сизова Г.В. Использование маркетинговой информации при оценке целесообразности инвестиций в объекты бытового обслуживания // «Маркетинг в России и за рубежом» - 2005. - № 4.
5. Погребова Е.С. Определение проблем развития бытового обслуживания в крупном городе посредством маркетинга // В сб. трудов «Региональный маркетинг сферы услуг». М.: МГУ сервиса, 2001. — С. 127—132.
6. Голобородько А.Ю. Оцінка регіонального розвитку сфери побутових послуг // Торгівля і ринок України: тематичний збірник наукових праць, Вип. 30, т.2 – Донецьк: ДонНУЕТ, 2010. – С. 120 – 127.
7. Офіційний веб-портал Київської міської влади [Електронний ресурс]. – Режим доступу: <<http://www.kmv.gov.ua/>>.
8. Офіційний веб-портал Святошинської районної у м. Києві державної адміністрації [Електронний ресурс]. – Режим доступу: <http://www.svyatoshin.kyiv-city.gov.ua/?area_id=105>.
9. Офіційний веб-портал Шевченківської районної у м. Києві державної адміністрації [Електронний ресурс]. – Режим доступу: <<http://shev.gov.ua/>>.
10. Сайт Департаменту підприємництва та споживчого ринку Харківської міської ради [Електронний ресурс]. – Режим доступу: <<http://uprcity.kharkov.ua/news/1048>>.
11. Національний класифікатор України «Класифікація видів економічної діяльності» ДК 009:2005, прийнятий наказом Держспоживстандарту України від 26 грудня 2005 р. N 375, чинний від 01.04.2006 р.

65. 012. 8:005

*Білецька І.М., к.е.н., доцент,
Козин Л.В., викладач,
Івано-Франківський інститут менеджменту
Тернопільського національного економічного університету*

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В СУЧАСНИХ УМОВАХ

Сучасна ринкова економіка дає можливість господарюючим суб'єктам самостійно визначати варіанти організації виробництва і можливості реалізації продукції, шляхи розвитку їх економічних інтересів, обирати партнерів по бізнесу. Це, у свою чергу, вимагає від них відповідальності за результати діяльності і обумовлює необхідність самостійного вирішення проблем безпечного і стійкого розвитку. З одного боку, в динамічних умовах розвитку глобальної економіки наростання невизначеності підприємницького середовища ускладнює функціонування механізмів ринкової саморегуляції; з іншого – пролонгований вплив не завжди ефективних та продуманих важелів державного контролю ринкових процесів роблять звичними для національної економіки такі явища, як несумлінна конкуренція, промислове шпигунство, створення «штучних» вхідних бар'єрів у ту чи іншу галузь народного господарства тощо. У таких умовах для вітчизняних підприємств особливо актуально постає проблема пошуку ефективних способів підвищення рівня забезпечення економічної безпеки діяльності.

Проблемам формування системи економічної безпеки підприємства та чинникам, що впливають на неї, присвячені роботи зарубіжних та українських вчених, зокрема Б. Анан'єва, А. Асмолова, Н. Бердяєва, Е. Соловійова, Р.Яновського, Г. Осипова, В. Серебрянникова, Є. Олейнікова, Т. Клебанової, З.Варналія, Т. Пастернак-Таранущенко та ін. Проте, низка аспектів стосовно особливостей побудови системи економічної безпеки підприємства і на сьогодні залишаються поверхнево дослідженими.

Метою публікації є визначення ключових аспектів процесу побудови системи економічної безпеки підприємства в сучасних умовах функціонування.

Питання визначення змісту економічної безпеки – складне та багатогранне, єдиного підходу до розуміння сутності даного поняття немає. Так, В.І. Забродський визначає сутність економічної безпеки як кількісну та якісну характеристику властивостей компанії, що відображає її здатність до «самовиживання» та розвитку в умовах виникнення зовнішнього чи внутрішнього ризику [1].

На думку В.В. Шликова, економічна безпека підприємства – це стан захищеності життєво важливих інтересів підприємства від реальних і потенційних джерел небезпеки або економічних загроз [2]. На думку Васильціва Т.Г., економічну безпеку підприємства можна розглядати як стан, за якого «підприємство і його продукція є конкурентоспроможними на ринку та одночасно гарантуються: найбільш ефективне використання ресурсів, інтелектуального та кадрового потенціалу; стабільність функціонування, стійкість та прогресивність розвитку; можливість протидіяти негативним впливам зовнішнього і внутрішнього середовища його функціонування» [2].

Таким чином, економічна безпека підприємства є водночас передумовою і наслідком ефективного функціонування підприємства в умовах загострення конкурентної боротьби на будь-якому з споживчого чи промислового ринків, особливо сьогодні – в умовах стабільно хиткого стану світової економіки.

У відповідності до Господарського Кодексу України, підприємство є самостійним суб'єктом господарювання, створеним компетентним органом державної влади або органом місцевого самоврядування (або іншими суб'єктами) для задоволення суспільних та особистих потреб через систематичне здійснення виробничої, науково-дослідної, торговельної, іншої господарської діяльності [3].

Усі заходи, спрямовані на забезпечення такого стану повинні ув'язуватися у єдину концепцію економічної безпеки підприємства – систему поглядів, помислів, що визначають основний напрям, стратегію і тактику реалізації бізнесово-підприємницьких проектів та програм [4].

На жаль, для більшості вітчизняних підприємств сьогодні поняття економічної (корпоративної) безпеки обмежується тільки договором з охоронною фірмою та паралельним використанням електронних та технічних засобів захисту корпоративної інформації. При цьому керівники підприємств у більшості не усвідомлюють, що це лише поодинокі елементи системи безпеки підприємства, при чому, як правило, вони є останньою лінією оборони.

Зазвичай, підприємства вирішують проблеми корпоративної безпеки локально, з точки зору окремих її елементів. Серйозно недооціненими залишаються цілі групи загроз для бізнесу.

Природно, що система безпеки підприємства залежить від багатьох чинників. По-перше, це вид бізнесу, у якому задіяне підприємство. Крім того, прямиий вплив на його економічну безпеку мають масштаб діяльності, наявність різних напрямів виробництва, офісних і виробничих потужностей у різних містах, регіонах чи країнах.

Загалом загрози щодо діяльності підприємства можна умовно поділити на зовнішні і внутрішні.

До зовнішніх прийнято відносити загрози, що можуть надходити з боку ділових партнерів, конкурентів, навколишнього середовища, криміналітету, політики уряду та органів державної і місцевої влади, бюрократії, форс-мажорних обставин тощо. Наприклад, контрагенти можуть бути умовно поділені у відсотковому співвідношенні на таких, що здатні завдати значної шкоди (41%), здатні завдати серйозної шкоди (22%), шахраїв (7%) і добросовісних партнерів (30%). Відсотки є приблизними, але в цілому співвідношення є справедливим.

На економічну безпеку підприємства мають вплив також політична ситуація, демографічні і соціальні тенденції в суспільстві. Наслідки світової економічної кризи, зміна формату міжнародних відносин, громадянський неспокій, локальні війни і конфлікти в тій чи іншій мірі відображаються на стані бізнесу в залежності від його масштабу та спрямованості. Соціальні загрози в основному стосуються страйків та епідемій. Політичні та міжнародні пов'язані з інфляцією, зміною торговельних і партнерських пріоритетів, введенням протекціоністських режимів, умовами ліцензування і патентування, націоналізацією тощо. Зокрема у Концепції економічної безпеки України виділені наступні макроекономічні загрози економічній безпеці:

невпевненість в довгострокових гарантованих поставках сировини і енергоносіїв за відсутності власних геологічних запасів і зростаючому подорожчання видобутку ключових корисних копалини;

технологічна залежність від передових країн світу в умовах створення ними штучних перешкод на шляху поширення досягнень НТП;

фінансова залежність вітчизняної економіки від інших країн і міжнародних фінансових організацій;

діяльність тіньових структур, неконтрольований відтік за межі України інтелектуальних, матеріальних і фінансових ресурсів;

збереження системи прихованої дискримінації, політичного і економічного домінування, фактичне неприйняття впливовими колами розвинених країн принципу рівноправного партнерства, використання ними обстановки асиметричної залежності [5].

До чинників внутрішніх загроз включають дії акціонерів, співробітників, недоліки системи управління, порушення встановленого режиму захисту інформації з обмеженим доступом для сторонніх осіб, порушення порядку використання технічних засобів, інші порушення правил режиму безпеки, діловодства тощо, які створюють передумови для реалізації протиправних цілей зацікавлених фігурантів, низький рівень кадрового, організаційно-правового, інформаційно-аналітичного забезпечення управління потенційними ризиками як у контексті внутрішніх, так і зовнішніх загроз, а також інші недоліки бізнес-технологій.

Поділ персоналу з точки зору його безпеки може бути представлений наступним чином: лояльні співробітники (33%), працівники, здатні завдати невеликої шкоди (50%), здатні завдати серйозної шкоди (12%) і шахраї (5%). Звичайно, на підприємстві, що складається з двох або трьох осіб, ситуація виглядає дещо інакше. У цьому випадку і одна людина здатна завдати підприємству 100%-их втрат. Таким чином, однією з найвагоміших складових концепції економічної безпеки підприємства повинна стати побудова системи кадрової безпеки – «сукупності заходів, спрямованих на попередження негативних впливів на економічну безпеку підприємства з боку ризиків і загроз, пов'язаних з персоналом, його інтелектуальним потенціалом і трудовими відносинами в цілому» [6].

Загрози безпеці підприємства на практиці проявляються у вигляді різних цілеспрямованих дій проти компанії («атак»), наслідки яких можна структурувати у такі групи:

фінансові – незаконне привласнення матеріальних і нематеріальних засобів підприємства;

інформаційні – розголошення комерційних таємниць, подробиць переговорних процесів, компрометуючих відомостей, крадіжки, знищення або пошкодження інформації, документів і баз даних;

матеріальні – саботаж, пошкодження або знищення майна компанії;

фізичні – нанесення прямих збитків через порушення перебігу нормальної діяльності, гальмування або зрив процесів виробництва, переговорів, забезпечення виконання договірних зобов'язань, загрози для здоров'я і життя керівників і персоналу.

Такі наслідки можуть мати різний характер. Наприклад, крадіжка інформаційних систем найчастіше пов'язана з хакерами ззовні, але при цьому не можна ігнорувати внутрішні фактори, такі як помилки у побудові системи інформаційної безпеки, навмисні або ненавмисні дії співробітників. Аналіз показує, що відсоток кібер-атак, що мали на меті зловмисну крадіжку або знищення інформації, є нижчим за 20%. Недооціненими залишаються й загрози, пов'язані з засобами соціальної інженерії. Керівництво не повинно ігнорувати небезпеку незаконного прослуховування телефонних розмов, які часто використовуються як професіоналами, так і аматорами, авантюристами і неробами завдяки високій поширеності і низькій вартості засобів підслуховування.

Головне, що слід враховувати – нема такої «атаки», яка б не використала інформацію або потурання інсайдерів. Це демонструє одну з найважливіших і найбільш вразливих складових системи безпеки підприємства – людський чинник. Отже, саме кадрова політика повинна привертати особливу увагу менеджменту, як в ролі потенційної загрози, так і у якості найбільш уразливої ланки. Кадрова безпека – категорія, яка є актуальною і вагомою на всіх рівнях від окремо взятого підприємства до національної економіки.

Як правило, кожна «атака» здійснюється в кілька етапів: формування намірів; збір інформації; аналіз даних; підготовка плану виділення необхідних ресурсів для реалізації запланованих кроків.

Іноді усе це – справа інтуїції і лічених секунд, а іноді – результат добре продуманого плану, що розроблявся кілька місяців або років, але обидва варіанти мають характерні ознаки кожної стадії, які можуть бути проаналізовані з метою запровадження профілактичних або захисних кроків.

Метою будь-якого підприємства є виявлення загроз, створення системи захисту активів, запобігання і припинення злочинів та інцидентів тощо. Корпоративна система безпеки повинна бути побудована таким чином, щоб забезпечити, у першу чергу, профілактику можливих загроз і атак. Цьому сприяє збір своєчасної і достовірної інформації про зовнішнє середовище, внутрішньої інформації, контррозвідувальна діяльність, аналіз отриманої інформації і на цій основі – визначення основних напрямів і рівнів загрози, тобто аналіз ризиків.

Якщо під ризиком узагалі розуміється «подія або група споріднених випадкових подій, що завдають збитку об'єкту, що володіє даним ризиком» [7], то під економічним ризиком мається на увазі «певна можливість виникнення збитків, які вимірюються в грошовому виразі» [8].

Загалом, ризик – це невизначеність бізнес-ситуації, яка має певну вірогідність нанести підприємству матеріальних (фінансових) та моральних (втрата або погіршення іміджу) збитків. Управління ризиками є основним видом діяльності системи корпоративної безпеки. Саме воно дозволяє реалізувати програму профілактики загроз і атак. Попередження злочину чи нещасного випадку набагато корисніше, ніж їх розкриття. Превентивна діяльність дає можливість економити кошти, а не витратити їх на незаплановані прості і менш ефективну діяльність у випадку виникнення загрозливих ризикових ситуацій.

На наш погляд, алгоритм побудови системи економічної безпеки підприємства повинен включати наступні етапи:

- 1) вивчення специфіки бізнесу підприємства, його ринкового сегменту, штатного розкладу, персоналу компанії;
- 2) аналіз зовнішніх і внутрішніх загроз діяльності підприємства;
- 3) дослідження історії виникнення кризових ситуацій, їх причин і наслідків розв'язання;
- 4) проведення аудиту діючих заходів із забезпечення безпеки і аналіз їх відповідності виявленим загрозам;
- 5) моделювання нової системи економічної безпеки підприємства та складання її бюджету;
- 6) впровадження системи безпеки у діяльність підприємства;
- 7) експертна оцінка дієвості побудованої системи та її системне вдосконалення.

Корпоративна система безпеки повинна бути в змозі протидіяти всьому спектру загроз. Так, система охоронної сигналізації та розміщення охоронців не може вирішити проблему розголошення таємниць компанії, збитків від діяльності корумпованих посадових осіб або загрози поглинання іншими організаціями. З іншого боку, ефективна система сигналізації і охорони може запобігти атакам з боку кримінального контингенту або змусити утриматися від ворожих дій нелояльних співробітників. Отже, кожен елемент системи корпоративної безпеки повинен мати чітке функціональне призначення, бути взаємопов'язаним з іншими і ефективно реагувати на потенційні і реальні загрози. Необґрунтована розбудова заходів безпеки може суттєво перешкоджати повсякденній діяльності, відволікати фінансові та людські ресурси. Натомість, погана організація системи безпеки, що неспроможна оцінити реальний рівень загрози, є надзвичайно небезпечною, оскільки дає помилкове відчуття безпеки і впевненості.

Таким чином, можна зробити висновок, що економічну безпеку підприємства треба розглядати в контексті практичного використання таких принципів сучасного менеджменту, як адекватна реакція на зміни в зовнішньому середовищі, правильна оцінка самого підприємства та його «вузьких місць», а також основних положень сучасної теорії менеджменту – системного та ситуаційного підходу до управління, що забезпечує адаптацію підприємства до умов його існування. Добре налагоджена система економічної безпеки діяльності підприємства дозволяє успішно реалізувати одне з правил Аристотеля Онассиса: «увесь секрет успішного бізнесу полягає в тому, щоби знати щось таке, що невідоме нікому іншому», адже вона надає можливість менеджеру дізнатися багато нового і про власну компанію, і про середовище, що її оточує.

Література

1. Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: Монографія / Т. Г. Васильців. – Львів: Арал, 2008. – 384с.
2. Экономическая безопасность / [Архипов А. И., Белоусов Р. А., Быков А. Н. и др.]; под ред. В. К. Сенчагова. – Москва: ЗАО «Финстатинформ», 1998. – 621с.
3. Господарський кодекс України: зі змінами і допов. станом на 18 січ. 2011 р.: (відповідає офіц. текстів) – К.: Правова єдність, 2011. – 159 с. – (Законодавство України).
4. Основи економічної безпеки : [Підруч. для вищ. навч. закл.] / О. М. Бандурка, В. Є. Духов, К. Я. Петрова, І. М. Червяков; Нац. ун-т внутр. справ. – Х., 2003. – 235 с.
5. Концепція економічної безпеки України / НАН України. Ін-т екон. прогнозування; [Викон.: Недін І. В. та ін.] – К.: Логос, 1999. – 55, [1] с.
6. Митрофанов А. А. Экономическая безопасность коммерческих предприятий и деловая разведка / А. Митрофанов. – [Електронний ресурс]. – режим доступу до сайту: <http://www.rscip.ru/base/A9738409-3441822.html>, вільний
7. Лашенко О. Кадрова безпека як підсистема в системі економічної безпеки підприємства / О. Лашенко. – [Електронний ресурс]. – режим доступу до сайту: www.nbu.gov.ua/e-journals/PSPE/2007-3/Laschenko_307.HTM, вільний.
8. Чернова Г.В. Практика управления рисками на уровне предприятия [Текст] : учеб. пособ. / Г. В. Чернова. – СПб. : Изд-во "Питер", 2000. – 176 с.