ТРАНСФОРМАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЗАСТОСУВАННЯ БЕНЧМАРКІНГУ

К. е. н. Чупріна М. О.,
Шеховцова І. А.

Україна, м. Київ, Національний технічний університет України «Київський політехнічний інститут»

Abstract*. Proved that modern conditions of doing business in Ukraine till the vymohy osoblyvi determine its informatsiyno-komunikatsiynoho software. Proved chto informatsiyna security company will znahodytys on nalezhnomu level at zastosuvannya benchmarking only todi, koly informatsiyna skladova ekonomichnoyi security will be considered as an integral part of management protsesu pidpryyemstvom. The criteria to be met by information that stanovlyat konfidentsiynu informatsiyu and ohoroni be indicated chto is pryskorennya transformatsiynyh protsesiv in ekonomitsi country requires raising informatsiynoyi vidtyznyanyh security companies and rozroblennya osnovnyh pidhodiv funktsionalnyh till the analysis of its components. It is established that the protection informatsiyi at provedenni protsedury oznachaye security benchmarking partner companies from zovnishnih and internal destabilizing factors chto dozvolyaye efektyvno vykorystaty dosvid diyalnosti and takozh realize their material, and finansovyy kadrovyy potentsial. The general threat information provided in the process of benchmarking and protection of information resources, namely the use of secure transmission channels benchmarking information; Control of the process; transmission of information is encrypted; the use of anti-virus protection, duplication of information in different media; the availability of clear rules and algorithms to work with information, briefing staff who work with benchmarking information; provide clear identification of the company that provides information during benchmarking. Proved that the development of further research in this area should be to assess possible factors reducing information security certification and improvement of systems and information security.*

Специфіка діяльності вітчизняних підприємств визначає особливі вимоги до їх інформаційно-комунікаційного забезпечення. Інформаційно-комунікаційне забезпечення функціонування підприємств в сучасних умовах господарювання включає сукупність технічних, програмних, організаційних і управлінських засобів, що формують середовище кодування і передавання інформації всередині підприємства та обмін інформацією з його зовнішніми контрагентами, включаючи доступ та інтегрування до мереж загального і спеціального використання різних рівнів. Інформаційно-комунікаційне забезпечення функціонуванняі підприємств в умовах застосування бенчмаркингу об'єднує вищенаведені елементи і має на меті сформувати середовище прийняття управлінських рішень в частині розроблення, виробництва, реалізації та захисту інноваційної продукції. глибоко дослідили функції, загрози та методи. Зазначимо, що саме прискорення трансформаційних процесів в економіці країни вимагає підвищення рівня інформаційної безпеки відтизняних підприємств та розроблення основних підходів до аналізу її функціональних складових.

Теоретичним і прикладним аспектам вирішення багатогранних проблем інформаційної безпеки підприємств, присвячені праці Т. Васильціва, Н. Ващенка, О. Голубченка, Л. Донця, Є. Степанової, Т. Ткачука, Н. Шведи та ін. [1 – 6]. Віддаючи належне теоретичній та практичній цінності попередніх здобутків, існує потреба у системному дослідженні проблематики формування системи інформаційної безпеки підприємств при реалізації процесу бенчмаркінгу.

Основними цілями даної статті є аналіз стану інформаційного забезпечення підприємства в умовах застосування бенчмаркінгу, а також розроблення практичних рекомендацій щодо формування системи інформаційної безпеки підприємств в сучасних умовах господарювання. Основні наукові результати дослідження базуються на використанні загальнонаукових методів економічного дослідження: наукової абстракції, аналізу та синтезу.

У системі забезпечення безпеки все більшого значення набуває забезпечення інформаційної безпеки підприємства. Це пов'язано із зростаючим об'ємом інформації, що поступає, вдосконаленням засобів її зберігання, передачі та обробки. Переклад значної частини інформації в електронну форму, використання локальних і глобальних мереж створюють якісно нові загрози конфіденційної інформації. Особливого значення набувають питання захисту інформації саме при проведенні процедури бенчмаркінгу. Бенчмаркінг розглядається науковцями як інноваційна технологія управління, яка дозволяє, на основі критичної оцінки внутрішнього і зовнішнього середовища досліджуваного підприємства та вивчення практики ведення бізнесу іншими успішними компаніями, створити безперервну систему удосконалень, що спрямовані на підвищення ефективність бізнесу досліджуваного підприємства за рахунок оригінальних управлінських, організаційних, маркетингових та фінансових дій та рішень [4].

Характерною ознакою бенчмаркінгу є наявність наукових досліджень і розробок, це творчий процес, який здійснюється на систематичній основі з метою збільшення обсягу знань, зокрема знань людини, культури та суспільства, і використання цього запасу знань в розробці нових пропозицій. Окрім наукових досліджень і розробок під час бенчмаркінгу реалізуються технічні, комерційні та фінансові дії, необхідні для виробництва нових або вдосконалених продуктів чи послуг і комерційного використання нових чи вдосконалених процесів.

Основним ресурсом, який дозволяє проводити сам бенчмаркінговий процес, є інформація. Окрім того, що для проведення бенчмаркінгу потрібно багато внутрішньої інформації, потрібна і зовнішня інформація, при отриманні якої існує багато різних проблем. І не останню роль при цьому відіграє процес захисту конфіденційної інформації обох партнерів. Отже, відомості, які становлять конфіденційну інформацію і підлягають охороні, повинні відповідати таким критеріям:

– їх відкрите використання пов'язане зі збитками для підприємства;

– вони не є загальновідомими або загальнодоступними на законних підставах;

– підприємство може вжити заходів для збереження їхньої конфіденційності з огляду на економічну та іншу вигоди;

– ці відомості потребують захисту, оскільки вони не є державними таємницями і не захищені авторським і патентним правом;

– приховування цих відомостей не зашкодить суспільств [2, 3].

До загроз інформації, яка надається у процесі бенчмаркінгу, на нашу думку, можна віднести: несанкціонований доступ підприємств або фізичних осіб, які проводять конкурентну розвідку; перехоплення інформації у каналах зв'язку; крадіжка інформації; пошкодження, знищення, повна втрата інформації; помилки при здійсненні аналітичного опрацювання інформаційних ресурсів; фальсифікація повідомлень.

Правове регулювання обігу інформації на підприємстві та відповідальності за правопорушення у зазначеній сфері ґрунтується на тому, що за українським законодавством захисту підлягає будь-яка документована інформація, неправомірне звернення до якої може завдати збитку її власникові, користувачеві. Захист здійснюється в цілях витоку, розкрадання, втрати, спотворення, підробки інформації, а також відвертання несанкціонованих дій зі знищення, модифікації, спотворення, копіювання, блокування інформації; відвертання інших форм незаконного втручання в інформаційні ресурси і інформаційні системи, забезпечення правового режиму документованої інформації як об'єкту власності. Крім того, за перелічені вище протиправні дії передбачена як адміністративна, так і кримінальна відповідальність. І це не випадково, оскільки загрози інформаційним системам можуть привести не лише до значних фінансових втрат, але і до безповоротних наслідків – ліквідації самого суб'єкта підприємництва. Також необхідно враховувати, що загроза інформаційним системам може настати з боку наступних суб'єктів:

- працівники підприємства, що використовують своє службове становище (коли законні права за посадою використовуються для незаконних операцій з інформацією);
- працівники підприємства, що не мають права в силу своїх службових обов'язків, але здійснили несанкціонований доступ до конфіденційної інформації;
- особи, які не пов'язані з підприємством трудовою угодою (контрактом).

За даними Міжнародної асоціації бенчмаркінгу [7] підприємства-партнери досить активно використовують різні засоби захисту інформаційних ресурсів, а саме: використання

захищених каналів передавання бенчмаркінгової інформації; проведення контролю процесу; передавання інформації у зашифрованому вигляді; використання антивірусного захисту, дублювання інформації на різних носіях; наявність чітких правил та алгоритмів роботи з інформацією, проведення інструктажу працівників, які працюють з бенчмаркінговою інформацією; забезпечення чіткої ідентифікації підприємства, що надає інформацію у процесі бенчмаркінгу.

Відтак, визнаємо, що інформаційна безпека підприємства буде знаходитись на належному рівні при застосування бенчмаркінгу лише тоді, коли інформаційна складова економічної безпеки буде розглядатися як невід'ємний елемент процесу управління підприємством. Проблема інформаційної безпеки має дуже загострений характер, оскільки разом з величезною кількістю методів захисту інформації, збільшується та урізноманітнюється кількість потенційних загроз і дестабілізуючих факторів. Захист інформації при проведенні процедури бенчмаркінгу означає захищеність підприємств-партнерів від зовнішніх та внутрішніх дестабілізуючих чинників, що дозволяє ефективно використати досвід діяльності, а також реалізувати їх матеріальний, фінансовий і кадровий потенціал.

Таким чином, можна зазначити, що розвиток подальших досліджень в даному напрямку повинен бути спрямований на оцінку можливих чинників зниження захищеності інформації та вдосконалення системи сертифікації систем та засобів захисту інформації.

ЛІТЕРАТУРА

1. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення : монографія / Т. Г. Васильців. – Львів : Арал, 2008. – 154 с.

2. Голубченко О. Л. Політика інформаційної безпеки / О. Л. Голубченко. – Луганськ : Вид. СНК ім. В. Даля. 2009. – 300 с.

3. Донець Л. І. Економічна безпека підприємства : навч. посібн. / Л. І. Донець, Н. В. Ващенко. – К. : Центр учбової літератури, 2008. – 240 с.

4. Шведа Н. М. Бенчмаркінг як технологія підвищення конкурентоспромроможності підприємства /Н. Шведа // Сталий розвиток економіки. – 2012. - №6 [16]. – с. 274-280.

5. Прокоф'єва Д. М. Підприємницьке шпигунство в системі інформаційних злочинів [Електронний ресурс] / Д. М. Прокоф'єва // Украинский центр информационной безопасности. – Режим доступу : www.bezpeka.com/library/lib_aspect.html

6. Ткачук Т. П. Формування системи інформаційної безпеки бізнесу / Т. Ткачук // Бізнес і безпека. – 2009. – № 4. – С. 19–23.

7. The most common data protection in the process of benchmarking (study 2014) [Електронний ресурс]/ Global Research Benchmarking. – Режим доступу: http://www.researchbench-marking.org/web/guest/home