УДК 338.4

СОРОКІВСЬКА Олена Анатоліївна,
кандидат економічних наук, доцент

ШВЕДА Наталія Михайлівна

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА В УМОВАХ ЗАСТОСУВАННЯ БЕНЧМАРКІНГУ

Здійснення бенчмаркінгу на підприємстві і використання його результатів в практичній діяльності є специфічним за змістом і комплексним за наслідками дослідженням. Правильно проведений бенчмаркінг дозволяє не тільки покращувати окремі аспекти функціонування підприємства, а й підвищувати його рівень конкурентоспроможності. Основним ресурсом, який визначає ефективність бенчмаркінгу та дозволяє оцінити якість процесу, є інформація. При проведенні бенчмаркінгу партнери повинні обмінюватися не лише відкритою та загальнодоступною інформацією, а й іноді і конфіденційною. В даній статті розглянуто особливості проведення бенчмаркінгу з точки зору дотримання інформаційної безпеки як підприємства-реципієнта, так і підприємства-донора. Автори пропонують принципи, на яких повинен ґрунтуватися обмін інформацією при здійсненні бенчмаркінгу, а також необхідні кроки для недопущення витоку конфіденційної та таємної інформації.

Ключові слова: *бенчмаркінг, інформація, інформаційна безпека, інформаційне середовище бенчмаркінгу, інформаційна структура бенчмаркінгу.*

Benchmarking at an enterprise and the practical usage of its results is the research that is distinctive in terms of content and complex in terms of consequences. If done correctly, benchmarking enables not only the improving of certain aspects of the enterprise functioning, but also the increasing of its competitiveness level. The main resource that allows measuring the benchmarking efficiency and accessing the process quality is information. When doing benchmarking, partners may have to share some confidential information rather than only the information that is open and available for general use. The peculiarities of benchmarking from point of view of information safety of both the recipient-enterprise and the donor-enterprise are considered in this article.
The authors offer some principles of sharing information when doing benchmarking as well as steps required to avoid the leak of confidential and secret information.

Keywords: *benchmarking, information, information safety, information environment of benchmarking, information structure of benchmarking.*

Постановка проблеми та її зв'язок з важливими науковими і практичними завданнями. Питання отримання, використання, поширення і збереження інформації в економіці і суспільстві в цілому набуває все

більшого значення. Від того, як організація використовує і захищає інформацію, залежить її виживання в ринковому середовищі. Сьогодні науковці достатньо глибоко дослідили функції, загрози та методи визначення рівня інформаційної безпеки підприємства в умовах трансформаційних процесів, розробили основні підходи до аналізу її функціональних складових. Проте проблема формування системи інформаційної безпеки підприємств при реалізації процесу бенчмаркінгу залишається малодослідженою.

Аналіз досліджень і публікацій. Методологічні, методичні та прикладні питання інформаційної безпеки підприємства висвітлені в наукових працях: В. Алена, Б. Андрушківа, О. Ареф'євої, О. Барановського, Б. Губського, Т. Васильціва, Т. Власюка, П. Войнаренка, Дж. Вуда, О.М. Джужі, Я. Жаліло, Д. Зеркалова, С. Ілляшенка, І. Керницького, Д. Ковальова, Г. Козаченко, Т. Кузенко, М. Куркіна, В. Мартинюка, Н. Метеленко, В. Михайленка, В. Нижника, Е. Олейникова, В. Ортинського, В. Понікарова, В. Пономарьова, К. Річардса, С. Сидоренка-Стеценка, А. Сухорукова, В. Тамбовцева, В. Франчука, О. Шнипко, О. Яременко та ін.

Зусиллями згаданих учених запропоновано економічні, інституційні та правові засади організації інформаційної безпеки підприємства, виділено основні принципи і напрями вдосконалення та створення системи інформаційної безпеки підприємства.

Метою дослідження є здійснення аналітичного оцінювання стану та перспектив інформаційного забезпечення процесу бенчмаркінгу, а також розроблення практичних рекомендацій щодо утримання достатнього рівня інформаційної безпеки партнерів по бенчмаркінгу.

Виклад основного матеріалу дослідження із обґрунтуванням одержаних результатів. Бенчмаркінг – це інноваційна технологія управління, яка на основі критичної оцінки внутрішнього і зовнішнього середовища досліджуваного підприємства та вивчення практики ведення бізнесу іншими успішними компаніями, котрі працюють як на аналогічному ринку, так і за його межами, дозволяє створити безперервну систему удосконалень, що покликана підвищити ефективність бізнесу досліджуваного підприємства на основі оригінальних управлінських, організаційних, маркетингових та фінансових дій та рішень [8].

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.

Прозорість та захищеність інформації при здійсненні процесу бенчмаркінгу нагадує єдність і боротьбу протилежностей. З одного боку, розкриття інформації про діяльність успішного підприємства дозволяє іншим фірмам оцінити результати цієї діяльності та порівняти із власними результатами, а підприємству-донору – покращити свій імідж, поділитись позитивним досвідом та отримати додатковий стимул для розвитку [5, 6]. Партнерам по бенчмаркінгу потрібна доступна, регулярна і надійна інформація для здійснення процесу порівняння перспектив і загроз подальшого розвитку та винесення компетентних рішень про підвищенню рівня конкурентоспроможності, що є можна визначити як кінцеву мету бенчмаркінгу.

З іншого боку, зайва відкритість інформації при проведенні бенчмаркінгу може завдати шкоди підприємству-донору, вступити в протиріччя з інтересами власників, управлінців і працівників, розкрити конфіденційну інформацію і комерційну таємницю. У зв'язку з цим досягнення балансу між захищеністю (відкритістю) та розповсюдженням (прозорістю) інформації стає діючим механізмом управління бенчмаркінгом у ринкових умовах.

Основними принципами надання інформації про підприємство у процесі бенчмаркінгу є:

– регулярність надання (одноразова передача інформації чи надання інформації з певною періодичністю, що залежить від необхідності при здійсненні бенчмаркінгу);

– оперативність надання (період часу від запиту на інформаційні ресурси до моменту їх надання);

– доступність для акціонерів та інших зацікавлених осіб;

– надійність інформації (джерело отримання інформації);

– повнота її змісту (повний або вибірковий (цільовий) масив інформаційних ресурсів);

– рівні права при наданні бенчмаркінгової інформації для усіх груп одержувачів.

Методи опрацювання інформації у системі відносин бенчмаркінгу реалізуються за допомогою інформаційного середовища, що створюється інформаційною структурою. Інформаційне середовище бенчмаркінгу є сукупністю технічних засобів, методів і способів руху інформації в організаційній системі, каналів та потоків її розповсюдження. Основна мета інформаційного середовища бенчмаркінгу – це формування відповідних баз документів і реалізація інформаційних відносин між донором та реципієнтом. Інформаційна система бенчмаркінгу повинна охоплювати всі основні показники діяльності організації, що піддаються формалізації.

Інформаційна структура бенчмаркінгу – це організована і керована взаємодія людей, технічних засобів, програмного забезпечення, даних і системних ресурсів, що збирають, перетворюють і поширюють інформацію у процесі бенчмаркінгу. Ключові поняття цього визначення охоплюють:

1. Людські ресурси. У передачі інформації у процесі бенчмаркінгу беруть участь як кінцеві користувачі, так і фахівці зі створення й експлуатації інформаційної системи. Кінцеві користувачі використовують інформаційну систему або інформацію, що у процесі бенчмаркінгу ця система створює. Фахівцями є люди, що розробляють інформаційні системи і приводять їх у дію.

2. Технічні ресурси. До них відносимо усе технічне обладнання і матеріали, які використовуються в обробці інформації у процесі бенчмаркінгу. До технічних ресурсів доцільно віднести не тільки комп'ютери й інше устаткування, але й усі носії даних, тобто всі матеріальні об'єкти, на яких ці дані записуються, — від паперу до магнітних дисків.

3. Програмні ресурси. Це сукупність програм, що забезпечують функціонування комплексу технічних засобів у процесі бенчмаркінгу. Універсальна концепція програмного забезпечення включає базовий (операційні системи, сервісні програми, транслятори) і прикладний (бази даних, експертні системи, редактори, електронні таблиці і т.п.) рівні.

4. Ресурси даних. Ресурси даних інформаційних систем організовані в бази даних, що зберігають створені й опрацьовані бази даних і знань. Тут у різноманітних формах містяться знання, такі, як факти, правила і приклади випадків успішного застосування ділової практики, особливості організації окремих процесів тощо.

5. *Мережні ресурси.* Телекомунікаційні мережі типу Інтернет, Інтранет та Екстранет стали необхідними для успішних дій усіх типів організаційних і інформаційних систем. Системні ресурси включають засоби зв'язку і мережну підтримку проведення бенчмаркінгу.

Будь-яка зацікавлена особа має право на отримання інформації про діяльність підприємства. Іноді з таким правом сполучається обов'язок суспільства надавати інформацію на запит зацікавленої особи. Наприклад, Закон «Про акціонерні товариства» зобов'язує акціонерне товариство на вимогу акціонера надавати йому для ознайомлення річні баланси, звіти товариства про його діяльність, протоколи зборів, документи, пов'язані з порядком денним зборів, книги протоколів засідань правління і т.п. [2]. Проте зацікавленій особі, як правило, надається відкрита (т. зв. публічна) інформація. До специфічної інформації, в тому числі з обмеженим доступом, дана особа не має доступу. І саме із специфічної інформації підприємство-реципієнт може отримати найбільшу користь при проведенні бенчмаркінгу. При здійсненні бенчмаркінгу основна проблема полягає в тому, щоб визначити яку саме інформацію можна надавати підприємству-партнеру, а яку – не варто ні за яких обставин (сюди відноситься інформація з обмеженим доступом).

Отже, інформація з обмеженим доступом поділяється на конфіденційну та таємну [3, 4]. Конфіденційна інформація – це інформація про фізичну особу (персональні дані) або юридичну особу, доступ та поширення якої можливі лише за згодою її власників (тобто тих, кого ця інформація безпосередньо стосується) та на тих умовах, які вони вкажуть.

Таємна інформація – це інформація, що містить відомості, які становлять державну та іншу передбачувану законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Чинним законодавством встановлено кримінальну та адміністративну відповідальність за розголошення комерційної таємниці та конфіденційної інформації [7]. Крім того, підприємствам надано можливість притягати посадових осіб до відповідальності, передбаченої установчими документами підприємства.

З метою забезпечення прозорості та ефективності проведення бенчмаркінгу підприємство, що надає інформацію, у своїх внутрішніх нормативних документах повинно визначити:

– перелік інформації, віднесеної до конфіденційної і таємної категорій (склад і обсяг відомостей);

– перелік осіб, що мають право доступу до інформації кожної з категорій;

– перелік осіб, що мають право класифікувати інформацію за режимом доступу;

– права й обов'язки посадових осіб щодо отримання, використання, поширення і збереження інформації з обмеженим доступом;

– відповідальність за забезпечення збереження інформації з обмеженим доступом.

Таким чином, підприємство повинно врегулювати у своїх внутрішніх документах питання отримання, поширення, використання і збереження інформації, в тому числі і такої, котра буде застосовуватися у процесі бенчмаркінгу.

Крім законодавчих і організаційних обмежень, поняття захищеності тісно пов'язано із засобами комунікацій, переважним використанням сучасних комп'ютерних систем і мереж в інформаційному забезпеченні організації. Найбільш імовірні загрози для цілісності інформації, яка надається у процесі бенчмаркінгу, і найбільш розповсюджені заходи захисту наведено в табл. 1.

За даними Міжнородної асоціації бенчмаркінгу [9] підприємства-партнери досить активно використовують різні засоби захисту інформаційних ресурсів (рис. 1).

Таблиця 1. Загрози та можливі засоби захисту інформації у комп'ютерних мережах при здійсненні процесу бенчмаркінгу.

№ з/п	Загрози інформації, яка надається у процесі бенчмаркінгу	Можливі засоби захисту
1	Несанкціонований доступ підприємств або фізичних осіб, які проводять конкурентну розвідку	Використання захищених каналів передавання бенчмаркінгової інформації, проведення контролю процесу доступу до інформації
2	Перехоплення інформації у каналах зв'язку	
3	Крадіжка інформації	Передавання інформації у зашифрованому вигляді
4	Пошкодження, знищення, повна втрата інформації	Використання антивірусного захисту, дублювання інформації на різних носіях
5	Помилки при здійсненні аналітичного опрацювання інформаційних ресурсів	Наявність чітких правил та алгоритмів роботи з інформацією, проведення інструктажу працівників, які працюють з бенчмаркінговою інформацією
6	Фальсифікація повідомлень	Забезпечення чіткої ідентифікації підприємства, що надає інформацію у процесі бенчмаркінгу

Так, найпоширенішим засобом захисту інформаційних ресурсів при проведенні бенчмаркінгу є використання захищених каналів передавання бенчмаркінгової інформації (99% із 100% опитаних підприємств-партнерів) та використання антивірусного захисту (98% із 100% опитаних підприємств-партнерів). Досить рідко проводиться ретельний інструктаж працівників, які працюють з бенчмаркінговою інформацією (лише 12% із 100% опитаних підприємств-партнерів) та забезпечується чітка ідентифікація підприємства, що надає інформацію у процесі бенчмаркінгу (28% із 100% опитаних підприємств-партнерів).

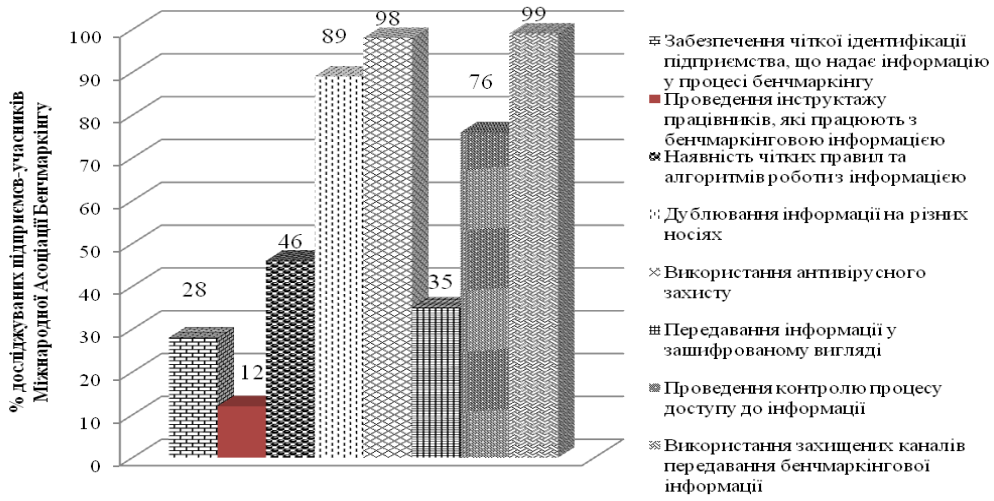

Рис. 1. Найпоширеніші засоби захисту інформації у процесі бенчмаркінгу. *Джерело: складено авторами на основі [9].*

Про необхідність використання сучасних засобів передачі інформації свідчить досить високий відсоток інфікування комп'ютерів вірусами та небезпечними програмами, які пошкоджують і знищують інформаційні ресурси (табл. 2).

Отже, на основі проведених досліджень можемо зробити висновок про зростаючий обсяг використання антивірусних програм та значну кількість випадків ураження комп'ютерної техніки небезпечними вірусами при роботі із нею.

Таким чином, забезпечення достатнього рівня інформаційної безпеки при проведенні бенчмаркінгу вимагає комплексних заходів, які повинні передбачати чітке розмежування таємної інформації та інформаційних ресурсів, які необхідно надати партнерам по бенчмаркінгу. Такі заходи захисту повинні виключати можливість витоку інформації з боку персоналу та технічних засобів.

Таблиця 2 – Динаміка використання антивірусних засобів захисту комп'ютерів у різних країнах.

Країна	Очищено комп'ютерів у I кварталі 2013 року	Очищено комп'ютерів у II кварталі 2013 року	Зміна, %
Україна	1 834 456	2 256 381	23,1
Росія	2 026 578	2 354 709	16,2
Білорусь	1 168 810	1 443 154	23,5
Франція	1 943 841	1 510 857	-22,3
Іспанія	1 358 584	1 348 683	-0,7
Велика Британія	1 490 594	1 285 570	-13,8

Джерело: складено авторами на основі [10]. Використовується показник під назвою "очищених компютерів на тисячу", що означає кількість комп'ютерів, очищених на кожну тисячу виконань спеціального утиліта для видалення шкідливих програм.

Висновки та перспективи подальших наукових досліджень. Таким чином, можемо стверджувати, що 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. Розуміння потреби захисту інформації, вибору надійних каналів її передавання, а також проведення своєчасного і ретельного інструктажу персоналу дозволить попередити та уникнути витоку інформаційних ресурсів, а також їх пошкодження та несанкціонованого знищення.

Список використаних джерел та літератури:

1. Економічна безпека: навч. посіб. /за ред. З.С. Варналія. – К.: Знання, 2009. – 647с.
2. Закон України «Про акціонерні товариства» (із змінами та доповненнями) від 17.09.2008 р. №514-VI [Електронний ресурс] – Режим доступу: http://www.kodeksy.com.ua/pro_aktsionerni_tovaristva.htm
3. Закон України «Про доступ до публічної інформації» (із змінами та доповненнями) від 13 січня 2011 року №2939-VI // Відомості Верховної Ради України. – 2011. - №32. – ст. 314.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (із змінами та доповненнями) від 05.07.1994р. №80/94-ВР [Електронний ресурс] – Режим доступу: http://www.zakon.rada.gov.ua/laws/show/80/94-вр
5. Кемп Р.С. Легальный промышленный шпионаж: Бенчмаркинг бизнес-процесов: технологии поиска и внедрения лучших методов работы ваших конкурентов. Пер. с англ. [Текст] / Р.С. Кемп; под ред. О.Б. Максимовой. – Днепропетровск: Баланс-Клуб, 2004. – 416 с.
6. Рейдер Р. Бенчмаркинг как инструмент определения стратегии и повышения прибыли: Пер. с англ. [Текст] / Р. Рейдер. — М.: РИА "Стандарты и качество", 2007. — 246с.
7. Цивільний кодекс України / Відомості Верховної Ради. – 2003. – №№ 40-44 [Електронний ресурс] – Режим доступу: www.rada.gov.ua
8. Шведа Н. Бенчмаркінг як технологія підвищення конкурентоспромроможності підприємства / Н. Шведа // Сталий розвиток економіки. – 2012. - №6 [16]. – с. 274-280.
9. The most common data protection in the process of benchmarking (study 2013) [Електронний ресурс]/ Global Research Benchmarking. – Режим доступу: http://www.researchbench-marking.org/web/guest/home
10. Dynamics of anti-virus protection of computers in different countries [Електронний ресурс]/ Kasperskylab. – Режим доступу: http://www.kaspersky.com/