Приятельчук О.А.*

ВПЛИВ КОРПОРАТИВНОЇ ЗВІТНОСТІ НА СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Кардинально отличительные, по сути и формам проявления, категории открытости корпоративной отчетности и обеспечения высокого уровня информационной безопасности предприятия являются достаточно взаимосвязанными понятиями. В этой статье автор осуществил попытку доказать их связь и оценить эффективность комбинации данных принципов в процессе корпоративного управления.

Ключевые слова: открытая корпоративная отчетность, защищенность информационной среды, концепция корпоративной социальной ответственности.

Кардинально відмінні за своєю суттю та формами прояву категорії відкритості корпоративної звітності та забезпечення високого рівня інформаційної безпеки підприємства є досить взаємопов'язаними поняттями. У даній статті автор здійснив спробу довести їх зв'язок та оцінити ефективність поєднання даних принципів в процесі корпоративного управління.

Ключові слова: відкрита корпоративна звітність, захищеність інформаційного середовища, концепція корпоративної соціальної відповідальності.

Totally different by their nature and forms categories of public corporate reporting and high condition of company's informational security have close interdependence. In this article the author has tried to demonstrate some kinds of connection between these categories and to evaluate the effectiveness of their combination in the process of corporate management.

Key words: public corporate reports, protection of informative environment, conception of corporate social responsibility.

В процесі обміну та використання інформаційних ресурсів підприємства виникає загроза відкриття комерційної інформації, яка може використатись в подальшому конкурентами та іншими представниками громадськості. На противагу даній загрозі відкритість корпоративної звітності, її оприлюднення та винесення на всезагальне обговорення (особливо складової, що стосується відрахувань на соціальні сфери, охорону навколишнього середовище, реалізацію благодійних та спонсорських проектів тощо) вже давно стало не лише необхідною об'єктивністю в зв'язку з регулюванням обов'язковості оприлюднення фінансової звітності у чітко визначених обставинах відповідними нормативними актами, а й додатковою вимогою, яка висувається до підприємств суспільством. На сьогодні відкрита корпоративна звітність є не лише елементом суворої фінансової звітності, а характеристикою відкритості, прозорості компанії, що впливає на формування її позитивного

* кандидат економічних наук, доцент кафедри міжнародного бізнесу Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

іміджу серед широкої громадськості та доброго ставлення з боку безпосередніх споживачів продукції.

В той же час, недоцільно нехтувати питаннями інформаційної безпеки підприємства. До останнього часу відношення керівників переважної кількості підприємств до питань побудови системи інформаційної безпеки підприємства та відкритості корпоративної звітності як елементу концепції корпоративної соціальної відповідальності було рівнозначно скептичним і сприймались виключно як додаткові видатки з досить невизначеними в майбутньому економічними ефектами. Однак відсутність втрат – це не прямий прибуток, оскільки збитки від розповсюдження комерційної інформації або створення негативного іміджу компанії можуть бути настільки значними, що витрати на утримання системи інформаційної безпеки та реалізацію соціальних проектів можуть бути значно нижчими за отримані переваги (у вигляді прибутку або нематеріальних цінностей).

За загальноприйнятими стандартами інформаційна безпека підприємства забезпечується наступними складовими, зокрема: 1) організацією нормативних документів на підприємстві – коли конкретні заходи та способи підвищення інформаційної безпеки закріплюються у відповідних посадових інструкціях, наказах і т.д., які, одночасно, регулюють і норми відповідальності за дотримання останніх; 2) операційні регулятори, що передбачають розробку методів та алгоритмів передачі та обміну інформації, взаємодію учасників даного обміну, їх можливості та рівень відповідальності; 3) програмно–технічними засобами, пов'язаними з розробкою, встановленням та використанням різноманітних технологічних засобів забезпечення інформаційної безпеки [2].

На нашу думку, дану систему слід доповнити ще однією складовою, актуальною в умовах необхідності дотримання певного рівня відкритості підприємства, що вимагається функціонуванням останнього в нових умовах інформаційного суспільства. Даним елементом слід вважати аналіз напрямків та об'єктів інформування, необхідного переліку документів, передбачених до розкриття, з метою пошуку балансу (компромісу) між відкритістю корпоративної звітності задля прозорості бізнесу та забезпечення належного рівня інформаційної безпеки.

Врахування необхідності відкритості деяких елементів корпоративної звітності в процесі побудови системи інформаційної безпеки на підприємстві може в деяких випадках бути використано і як антикризовий захід, оскільки інформаційна безпека в широкому розумінні передбачає не лише захист внутрішньої інформації, а й недопущення появи негативної інформації (чорного піару) з зовнішніх джерел. У кожної компанії потенційно існує загроза виникнення кризових ситуацій – вийшла партія недоброякісної продукції, провідні співробітники відзначились непристойною поведінкою або були опубліковані відомості щодо забруднення навколишнього середовища діями компанії. Інформаційна відкритість перед суспільством сприяє мінімізації негативних наслідків даних методів чорного піару.

Найчастіше відкритість компанії знаходить вираз у наданні засобам масової інформації необхідної інформації, у вичерпних коментарях, відкритості деяких елементів звітності та виразу готовності до діалогу та співробітництва. Саме такі заходи зможуть втримати задовільний рівень інформаційної безпеки. В даному випадку: попередити – значить контролювати – значить убезпечити.

З метою побудови системи (розробки засобів, технологій) захисту інформації конкретної інформаційної системи будується так звана політика інформаційної безпеки (політика безпеки інформації в організації), що передбачає сукупність документованих правил, процедур, практичних прийомів або принципів управління в сфері безпеки інформації, якими керується підприємство в своїй діяльності.

Метою побудови даної системи є досягнення стану інформаційної безпеки підприємства – тобто стану захищеності інформаційного середовища підприємства, забезпечення її формування, використання та розвитку. Але в сучасних умовах захищеність не повинна ототожнюватись з закритістю інформації, а, швидше за все, з «розумною» відкритістю інформації [1].

Інформаційну безпеку досить часто ототожнюють з поняттям інформаційно–технічної безпеки, де сферою створення загроз та застосування заходів безпеки є переважно новітні технології, програмне забезпечення тощо. В сучасному суспільстві виникає додатковий рівень інформаційної безпеки – інформаційно–психологічна (психофізична) безпека. Інформаційно–психологічна безпека трактується як стан захищеності окремих груп осіб (компаній) від негативного інформаційно–психологічного впливу та пов'язаних з цим інших життєво важливих інтересів особистості, підприємства, суспільства в цілому [5].

Інформаційно–психологічна безпека споживачів інформації є похідною інформаційної безпеки підприємства. Користувачі корпоративної звітності, в свою чергу, є системною складовою підприємства. Відкритість інформації сприяє забезпеченню надійного рівня їх інформаційної–психологічної безпеки, а, отже, опосередковано впливає й на загальний стан інформаційної безпеки підприємства.

Існує ще один критерій встановлення балансу між відкритістю корпоративної інформації, зокрема звітності, та забезпечення інформаційної безпеки підприємства – національні особливості, зокрема менталітет користувачів даної інформації. В силу цілого ряду обставин – менталітету, цінностей, особливостей історичного розвитку окремих країн тощо – у представників різних національностей (країн) сформувались часто кардинально відмінні оцінки відкритості компаній, соціальної орієнтації їх діяльності. Якщо розглядати вищеназвані методи діяльності підприємств як складові цілісної концепції корпоративної соціальної відповідальності, яка, зокрема, включає в себе такі елементи, як: прозорість ведення бізнесу, відкритість фінансової звітності, захист прав та інтересів споживачів та співробітників компанії, реалізація проектів в сфері охорони довкілля, соціальних проектів – будівництво об'єктів соціального призначення, дотація культури та освіти, благодійні та спонсорські програми тощо, можна використати результати досліджень вподобань населення (споживачів даної відкритої інформації) окремих національностей та країн світу.

Зокрема, щодо окремих складових концепції корпоративної соціальної відповідальності, у відповіді на запитання щодо важливості певних елементів, які враховує споживач в процесі формування думки про компанію–виробника та прийняття рішення щодо споживання даної продукції, 33% респондентів виділили захист навколишнього середовища зусиллями підприємства, 28% – інвестиції в соціальну сферу, 23% – відкритість корпоративної звітності (показники 2009 року; до того ж, у порівнянні з аналогічними показниками за 2006 рік значення кожного з вищеназваних критеріїв зросло в середньому на 2–15%).

61% респондентів (на противагу 50% у 2006 році) висловились за необхідність законодавчого закріплення відкритості корпоративної звітності з боку компаній – виробників споживчих товарів та послуг. Експерти, в свою чергу, рівень інформаційної безпеки компаній, що здійснюють подібне оприлюднення добровільно, оцінюють значно вище, оскільки останні не зазнають руйнівного впливу руху негативної інформації ззовні за умови закритості корпоративної звітності [3].

Щодо національних переваг, то найбільш сприятливими щодо даних параметрів діяльності компаній є громадськість країн з соціально–орієнтованою економікою, зокрема Швеція, Данія, Норвегія, Швейцарія, Німеччина, Японія і т.д.

Підводячи підсумки вищесказаному, можна дійти до висновку, що два таких поняття як відкритість корпоративної звітності та забезпечення інформаційної безпеки хоча й передбачають в оперативному плані кардинально відмінні цілі, значною мірою заперечуючи реалізацію одних іншими, однак в стратегічному плані слугують загальній меті – ефективній діяльності підприємства за умови належного рівня захисту інформації та одночасного створення позитивного іміджу прозорого бізнес–партнера та постачальника товарів або послуг кінцевим споживачам – представникам суспільства. До того ж, розумне використання подібної відкритості може слугувати навіть підвищенню рівня інформаційної безпеки.

Література

1. Е.А. Белокурова. Комментарий к Закону РФ «О безопасности» (постатейный). М.: 2008.
2. Информационная безопасность (2–я книга социально–политического проекта «Актуальные проблемы безопасного социума»). М.: «Оружие и технологии», 2009.
3. 2009 Survey report of consumer attitudes toward corporate responsibility, BITCI/Ipsos MORI, 2009. [Електронний ресурс] – Режим доступу: http://www.bitc.ie/corporate_responsibility/reporting.html
4. ISO/IEC 27001:2005 – «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования». Международный стандарт. [Електронний ресурс] – Режим доступу: http://www.am–soft.ua/site/page5077.html
5. ISO/IEC 27000 – Словарь и определения. [Електронний ресурс] – Режим доступу: http://iso27000.ru/standarty/iso–27000–mezhdunarodnye–standarty–upravleniya–informacionnoi–bezopasnostyu–1