

ренних бизнес-процессах предприятия и их структуре, раскрывает знания об элементах бизнеса, показывает логику создания ценности в бизнес-системе и условия обеспечения ее качества и раскрывает новые возможности бизнеса, которое в отличие от существующих подходов основывается на комплексном подходе к пониманию сущности данной категории.

Практическая значимость. Понимание сущности термина «бизнес-модель» и определение его ключевых аспектов является теоретическим основанием для определения целевых ориентиров развития предприятия, направленных на повышение эффективности его функционирования в трансформационных условиях хозяйствования.

Ключевые слова: бизнес-модель, концепция, эволюция, сущность, подходы.

Purpose. The aim is to study the theoretical aspects of the concept of the business model of the enterprise, and systematic research scientists' view on the interpretation of the essence of the term «business model».

Methods. The study used the method of analysis, synthesis and generalization.

Results. Based on this analysis, the main stages of the evolution of the concept of the business model of the enterprise, systematized the main approaches to the interpretation of the essence of this category and the author's definition proposed definition of «business model».

Scientific novelty. Developed further determine the nature of the business model – as a basis for competitive advantages, which describes the process of generating a profit, features a method of business organization, focuses on the internal business processes of the company and its structure reveals knowledge about the elements of business, shows the logic of value creation in business system and conditions to ensure its quality and opens up new business opportunities, which, in contrast to the existing approaches based on a comprehensive approach to understanding the essence of this category.

Practical relevance. Understanding of the term «business model» and the definition of its key aspects is the theoretical basis for determining the targets of the company to improve its efficiency in the transformation of economic conditions. Tags: business model, concept, evolution, nature, approaches.

Key words: business model, concept, evolution, nature, approaches.

Рекомендовано до публікації д-ром екон. наук,
проф. Фроловою Л.В. Дата надходження рукопису 29.11.2012 р.

УДК [005.4:004.78]:339.17

Ликова О.І.

Донецький національний університет економіки
і торгівлі імені Михайла Туган-Барановського,
м. Донецьк, Україна, e-mail: admin@study.dn.ua

АНАЛІЗ АУТСОРСИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Lykova O.I.

Donetsk National University of Economics and
Trade named after Mykhayilo Tugan-Baranovsky,
Donetsk, Ukraine, e-mail: admin@study.dn.ua

ANALYSIS OF OUTSOURCING INFORMATION SECURITY

Мета. Метою статті є аналіз аутсорсингу інформаційних технологій щодо інформаційної безпеки торговельного підприємства.

Методика. У процесі дослідження використано: методи теоретичного узагальнення та порівняння, аналізу й синтезу (для уточнення змісту поняття «аутсорсинг інформаційної безпеки»).

Результати. На підставі проведеного дослідження визначено поняття аутсорсингу інформаційної безпеки торговельного підприємства, сформульовані основні компоненти функціонування систем захисту інформації, зокрема DLP-систем (Data Loss Prevention). Також окреслені основні переваги та проблеми аутсорсингу, сформульовані критерії вибору компанії-аутсорсера, що здійснюватиме комплекс заходів з організації інформаційної безпеки.

Наукова новизна. Уточнено понятійний апарат аутсорсингу інформаційної безпеки торговельного підприємства, удосконалено науково-методичний підхід щодо критеріїв вибору компанії-аутсорсера в частині захисту комерційної інформації, запобігання проблемам, пов'язаним із несанкціонованим просоченням даних, що сприятиме посиленню інформаційної безпеки торговельного підприємства.

Практична значущість. Отримані результати спрямовані на оптимізацію системи захисту комерційної інформації, посилення інформаційної безпеки торговельного підприємства. Інфраструктура інформаційних систем торговельних мереж має свої специфічні особливості – масштабність і велику територіальну розподіленість, що може призвести до втрати важливих даних. Ураховуючи це, для забезпечення інформаційної безпеки обґрунтована необхідність залучення зовнішніх спеціалістів аутсорсингової компанії.

Ключові слова: інформаційна безпека, аутсорсинг, системи захисту інформації, DLP-системи.

В умовах розвитку сучасного інформаційного суспільства, а також посилення конкуренції та різкого скорочення витрат компаній підвищення ефективності вкладень у засоби забезпечення інформаційної безпеки стає одним з першочергових завдань.

Далеко не всі торговельні підприємства можуть дозволити собі мати в штаті службу фахівців з інформаційної безпеки, яка здатна самостійно вирішувати завдання в цій галузі на високопрофесійному рівні. Одним із найбільш перспективних варіантів у такій ситуації є передача цих функцій сторонній організації, яка спеціалізується на наданні цього виду послуг. Тобто, по суті, мова йде про аутсорсинг інформаційної безпеки підприємства.

Інформація для сучасного бізнесу часто має навіть більшу цінність, ніж матеріальні активи, – ризики потрапляння конфіденційних даних у чужі руки вкрай великі, а реалізація цих ризиків може призвести до зменшення вартості бізнесу або його повної втрати. Основною зброєю конкурентної боротьби стає використання інформації. В Україні законодавчо врегульовано загальні правові основи одержання, використання, поширення та зберігання інформації, закріплено право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначений статус учасників інформаційних відносин, доступ до інформації та її охорону [1; 2].

Згідно з дослідженнями аналітичного центру Zecurion Analytics, оцінюваний збиток від публічних інцидентів інформаційної безпеки в 2011 році перевищив 20 млрд дол (в середньому \$ 25,13 млн дол на кожен інцидент). При цьому були скомпрометовані персональні дані понад 350 млн чоловік. Найбільша кількість інцидентів (45,2%) відбувається внаслідок помилок або недбалості персоналу, низької поінформованості співробітників компаній з питань інфор-

маційної безпеки. Найбільше інформації просочується з медичних організацій (20,4%), держустанов (16,7%), освітніх закладів (15,2%), підприємств роздрібно-ї торгівлі (13,8%). Найчастіше інформація втрачається через ноутбуки та мобільні накопичувачі (сумарно 19,4%), веб-сервіси (18,2%), комп'ютери (16,1%), а також неелектронні носії (13,8%).

Питанням аутсорсингу присвячена достатня кількість наукових робіт у сучасній вітчизняній і західній економічній літературі. Це наукові дослідження таких авторів, як Д. Михайлов, П. Готтшальк, Б. Анікін, Е. Спарроу [3-6]. Інформаційну безпеку підприємства розглядали такі науковці, як В. Годін, І. Корнеєв, А. Курило, А. Шиверський [7-9]. Проте питання, пов'язані з процесами аутсорсингу щодо в частині інформаційної безпеки підприємства, вимагають подальшого більш глибокого вивчення й аналізу.

Аутсорсинг інформаційних технологій передбачає передачу сторонній організації повністю або частково функцій, пов'язаних з інформаційними технологіями підприємства, а саме: управління інформаційними системами, обслуговування мережевої інфраструктури, розміщення корпоративних баз даних на серверах спеціалізованих компаній і т. ін. [5; 6]

Аутсорсинг інформаційної безпеки підприємства – це передача на підставі договору певних бізнес-процесів або функцій, пов'язаних з безпекою інформаційних ресурсів, на обслуговування сторонній компанії, що спеціалізується у відповідній галузі. Отже, стороння компанія адаптує власні внутрішні ресурси і знання під потреби бізнесу та використовує їх в інтересах конкретного замовника. На відміну від послуг сервісу і підтримки, що мають разовий характер, аутсорсинг базується на основі довготривалого контракту [4].

Метою статті є аналіз аутсорсингу інформаційних технологій щодо інформаційної безпеки торговельного підприємства.

Термін «інформаційна безпека» має декілька визначень. В основному вони стосуються технічної специфіки діяльності та охоплення загальної кількості напрямків, у межах яких здійснюється захист. Однак усі визначення ототожнюють безпеку як діяльність, безпосередньо спрямовану на припинення просочення інформації за межі інформаційної системи торговельного підприємства або ж запобігання несанкціонованій трансформації даних.

Згідно із Законом України «Про інформацію» захисту підлягає інформація, володіння якою дає змогу її дійсному чи потенційному власнику одержати вигаш моральний, матеріальний чи політичний [1].

Так, відповідно до [7], інформаційна безпека – захищеність інформації на будь-яких носіях від випадкових і навмисних впливів природної або штучної властивості, спрямованих на знищення, видозміну тих чи інших даних, зміну ступеня доступності цінних відомостей.

Інші експерти [8] дають таке визначення. Інформаційна безпека – один з видів безпеки, що визначається через «стан захищеності», зокрема впевненості та довіри в безпеці. Ця впевненість орієнтована на соціум – людину або групу осіб, які очікують або ж прагнуть досягти деяких цілей і що роблять в цьому зв'язку якісь дії. В окремому коментарі в частині, що стосується безпеки мереж та інформаційних систем, підкреслюється: «Увесь бізнес являє собою питання

довіри. Довіра може розвинутися тільки в тому випадку, коли учасники угоди відчують надійність і безпеку».

Для забезпечення інформаційної безпеки торговельних підприємств використовуються спеціальні системи захисту інформації (СЗІ). Кожна окрема СЗІ являє собою цільний комплекс організаційних, технічних, технологічних, програмних та інших засобів, методів і заходів, що знижують уразливість інформації та перешкоджають несанкціонованому (незаконному) доступу до інформації, її просочення або втраті [9].

На думку багатьох експертів, однією з ключових проблем у цьому напрямку можна вважати просочення інформації, яка може становити комерційну цінність. Для боротьби з цим явищем використовуються системи захисту від просочення інформації – DLP (скорочено з англ. Data Loss Prevention).

На відміну від комп'ютерних антивірусних програм, завдання DLP-системи – захист корпоративної інформації від спроб передачі її в руки конкурентів. Організувати крадіжку та подальшу передачу (продаж) комерційно значущих даних можуть конкуренти, використовуючи з цією метою персонал підприємства. Іншою причиною просочення може бути людський фактор – банальна неуважність, ігнорування прийнятих норм безпеки, а також незнання таких.

Згідно з рисунком 1, більшості випадків експерти визначають такі рішення, які відносяться до DLP.

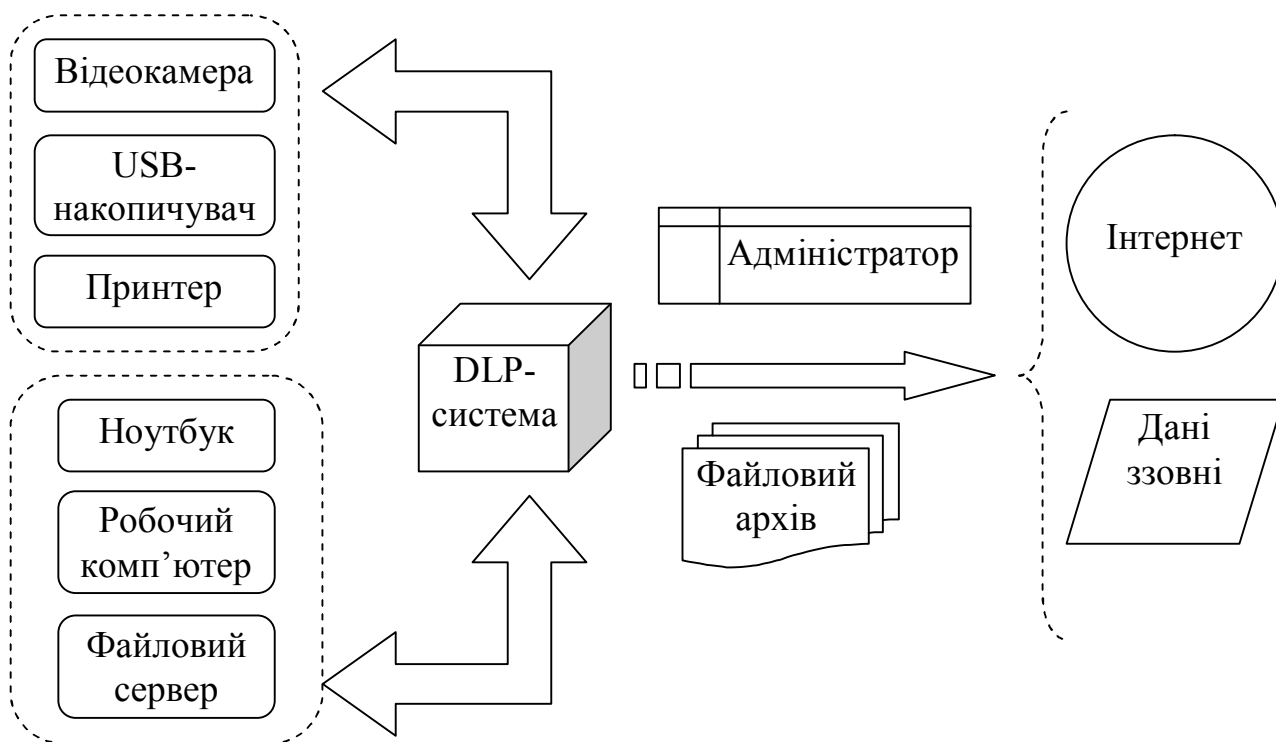


Рисунок 1 – Схема функціонування DLP-системи

1. Максимально повний контроль усіх відомих каналів просочення інформації.

Сюди входить контроль за інтернет-каналами – сайтами (у тому числі соціальними мережами), чатами, електронною поштою тощо, а також іншими но-

сіями та накопичувачами інформації, не підключеними безпосередньо до мережі, – дисками, флеш-накопичувачами і т. ін.

До цієї ж групи можна віднести й мобільні телефони, в основі яких лежить стільниковий принцип радіозв'язку. Однак у випадку з телефонами застосовуються спеціальні методи (наприклад, системи заглушення радіосигналів), і це вже виходить за рамки ряду DLP.

До іншої групи можна віднести локальні пристрої – принтери, сканери і т. ін.

2. Організація моніторингу та аналіз інформації. Тобто мова йде про організацію контролю трафіка (інтернет) і переміщення інформації як такої (рух документації по офісу, робота з файлами, копіювання даних тощо).

Розпізнавання потенційних загроз просочення і їх максимально швидке блокування, виявлення осіб, причетних до таких незаконних дій. У разі виникнення нештатної ситуації система автоматично робить дії в межах встановлених регламентів, а також визначає робоче місце, з якого робиться спроба порушення.

3. Зберігання інформації. DLP-система завантажує всі необхідні дані в спеціальну базу даних до з'ясування причин, за якими система кваліфікувала ситуацію як потенційну загрозу.

Очевидно, що для підтримки життєзабезпечення всіх рішень з інформаційної безпеки підприємства необхідні високопрофесійні профільні фахівці. Причому ці фахівці повинні вже мати в своєму арсеналі спеціальні програмні комплекси та інформаційні системи, актуальні саме в цьому вузькоспеціалізованому сегменті. Тому для керівництва підприємства найбільш прийнятним рішенням є залучення зовнішніх фахівців аутсорсингової компанії.

Як правило, компанія-аутсорсер має набагато більший досвід у сфері встановлення обладнання та оперативного реагування на інциденти, що виникають. Причому, що вкрай важливо, будучи сторонньою організацією, аутсорсер може бути більш об'єктивним і не схильним до замовчування проблем через особисті пристрасті. У фінансовому плані наявність готових рішень з інформаційних технологій дозволить заощадити на дорогій розробці власного ПЗ з подальшим його тестуванням, доробкою, налаштуванням і супроводженням.

Надзвичайно важливою є проблема визначення критеріїв вибору компанії-аутсорсера, яка буде здійснювати весь комплекс заходів з організації інформаційної безпеки [10].

Тут слід звернути увагу на такі моменти:

- чітко визначені та відповідним чином задокументовані алгоритми дій щодо впровадження й подальшого супроводу ІБ торговельного підприємства;
- власна матеріально-технічна база та наявність необхідного обладнання
- володіння в достатній кількості власними ресурсами та можливостями (наприклад, можливість постійного чергування технічного персоналу);
- наявність власних програмних розробок у профільній сфері;
- присутність у компанії кваліфікованих (підтверджується сертифікатами) фахівців в технологічній і технічній сфері;
- наявність постійних клієнтів відповідного рівня, а також позитивні відгуки від цих клієнтів;
- угода про рівень надання послуги SLA (англ. Service Level Agreement);

- вартість упровадження та супроводу;
- можливі ризики, пов'язані з допуском у «секрети» фірми сторонніх людей.

Зменшення витрат на відповідну інфраструктуру можна вважати дуже серйозною перевагою, яку беруть до уваги, започатковуючи процес переведення інформаційної безпеки на аутсорсинг. Оптимізація фінансових потоків підприємства дозволяє акумулювати певні ресурси для розвитку основних напрямків бізнесу. Допомогає більш чітко і прозоро здійснювати фінансування та зменшувати зайві витрати. Зменшується навантаження на власних спеціалістів інформаційних відділів і відділів безпеки.

Однак прийняти позитивне рішення буває досить важко. Необхідність надання доступу до конфіденційної інформації спричиняє за собою складність прийняття рішення про аутсорсинг як таке, але й надалі – проблема визначення меж допуску не перестає бути актуальною. Звідси впливає і проблема контролю дій самих аутсорсерів. Наступною загрозою може стати мимовільне залучення підприємства в одвічне протистояння фахівців з інформаційної безпеки та їх власних антиподів – хакерів.

Щостосується практичного застосування систем захисту інформації, то як свідчить світовий досвід, воно має сенс для великих торговельних підприємств. Слід зазначити, що інфраструктура інформаційних систем торговельних мереж має свої специфічні особливості – масштабність і велику територіальну розподіленість. ІТ-інфраструктура ритейлерів – це серйозні обчислювальні потужності, офісні інформаційні системи, великі мережі передачі даних, різноманітні апаратні засоби для забезпечення логістики, обладнання магазину і торговельного залу. Отже в цьому випадку для забезпечення інформаційної безпеки потрібна професійно налагоджена система захисту комерційної інформації та посилена інформаційна безпека, що у свою чергу, потребує залучення зовнішніх експертів-аутсорсерів.

Висновки:

1. Визначено поняття аутсорсингу інформаційної безпеки торговельного підприємства як передачі на підставі договору відповідних бізнес-процесів або функцій, пов'язаних з безпекою інформаційних ресурсів, на обслуговування сторонній компанії, що спеціалізується у відповідній галузі.
2. Сформульовані основні компоненти функціонування систем захисту інформації, зокрема DLP-систем.
3. Окреслені основні критерії вибору компанії-аутсорсера, що має здійснювати весь комплекс заходів з організації інформаційної безпеки.

Список літератури/References:

1. Про інформацію [Електронний ресурс]: Закон України. – Режим доступу: <<http://zakon1.rada.gov.ua/laws/show/2657-12>>. Law of Ukraine, “About information”, available at: <http://zakon1.rada.gov.ua/laws/show/2657-12>.
2. Про захист інформації в автоматизованих системах: Закон України [прийнято ВР 5 лип. 1994 р.] // Закони України. – 1997. – Т. 7.

- Law of Ukraine (1997), "About defence of information in the automated systems", *Zakon Ukraine*, Vol. 7.
3. Михайлов Д.М. Аутсорсинг. Новая система организации бизнеса: учеб. пособие / Д.М. Михайлов. – М.: КНОРУС, 2009. – 256 с.
Mihailov, D.M. (2009), *Autosorsing. Novaya sistema organizatsii biznesa* [Aut-sorsing. New system of organization of business], KNORUS, Moscow, Russia.
 4. Готтшалк П. ИТ-аутсорсинг: построение взаимовыгодного сотрудничества / П. Готтшалк, Х. Солли-Сетер; пер. с англ. А. Петров, А. Сатунин. – М.: Альпина Бизнес Букс, 2007. – 390 с.
Gottshalk, P. and Solli-Seter, H. (2007), *IT-autosorsing: postroenie vzaimovygod-nogo sotrudnichestva* [IT-AUTSORSING: construction of mutually beneficial col-laboration], Translated by Petrov, A. and Satunin, A., Alpina Biznes Buks, Mos-cow, Russia.
 5. Аникин Б.А. Аутсорсинг и аутстаффинг: высокие технологии менеджмента / Б.А. Аникин, И.Л. Рудая. – М.: Инфра-М, 2006. – 288 с.
Anikin, B.A. and Rudaya, I.L. (2006), *Autosoring i autstaffing: vysokie tehnologii menedjmenta* [Aut-sorsing and autstaffing: high technologies of management], In-fra-M, Moscow, Russia.
 6. Спарроу Э. Успешный ИТ-аутсорсинг / Э. Спарроу; пер. с англ. Ю. Алабина. – М.: КУДИЦ-ОБРАЗ, 2004. – 288 с.
Sparroy, E. (2004), *Uspeshnyi IT-autsorsing* [Successful IT-autsorsing], Translated by Alabina, Yu., KUDIC-OBRAZ, Moscow, Russia.
 7. Годин В.В. Управление информационными ресурсами: 17-модульная про-грамма для менеджеров «Управление развитием организации». Модуль 17 / В.В. Годин, И.К. Корнеев. – М.: ИНФРА-М, 2000. – 352 с.
Godin, V. and Korneiev, I. (2000), *Upravlenie informacionnymi resursami* [Ma-nagement informative resources], INFRA-M, Moscow, Russia.
 8. Курило А.П. Аудит информационной безопасности / А.П. Курило [и др.]. – М.: БДЦ-пресс, 2006. – 304 с.
Kurilo, A.P. (2006), *Audit informacionnoi bezopasnosti* [Audit of informative safe-ty], BDC-press, Moscow, Russia.
 9. Шиверский А.А. Защита информации: проблемы теории и практики / А.А. Шиверский. – М.: Юрист, 1996. – 112 с.
Shiverskii, A.A. (1996), *Zashita informacii: problemy teorii i praktiki* [Defence of information: problems of theory and practice], Yurist, Moscow, Russia.
 10. Лаврухин А. Аутсорсинг информационной безопасности – «за» и «против» / А. Лаврухин // CONNECT. – 2012. – № 11. – С. 62-63.
Lavruhin, A. (2012), "Aut-sorsing of informative safety – «pro and con»", *CONNECT*, No. 11, pp. 62-63.

Цель. Целью статьи является анализ аутсорсинга информационных технологий от-носительно информационной безопасности торгового предприятия.

Методика. В процессе исследования использованы: методы теоретического обобще-ния и сравнения, анализа и синтеза (для уточнения содержания понятия «аутсорсинг ин-формационной безопасности»).

Результаты. На основании проведенного исследования определено понятие аутсорсинга информационной безопасности торгового предприятия, сформулированы основные компоненты функционирования систем защиты информации, в частности DLP-систем (Data Loss Prevention). Также очерчены основные преимущества и проблемы аутсорсинга, сформулированы критерии выбора компании-аутсорсера, что будет осуществлять комплекс мероприятий по организации информационной безопасности.

Научная новизна. Уточнен понятийный аппарат аутсорсинга информационной безопасности торгового предприятия, усовершенствован научно-методический подход относительно критериев выбора компании-аутсорсера относительно защиты коммерческой информации, предупреждения проблем, связанных с несанкционированной утечкой данных, что будет способствовать усилению информационной безопасности торгового предприятия.

Практическая значимость. Полученные результаты направлены на оптимизацию системы защиты коммерческой информации, усиление информационной безопасности торгового предприятия. Инфраструктура информационных систем торговых сетей имеет свои специфические особенности – масштабность и большую территориальную распределенность, что может привести к потере важных данных. Для обеспечения информационной безопасности обоснована необходимость привлечения внешних специалистов аутсорсинговой компании.

Ключевые слова: информационная безопасность, аутсорсинг, системы защиты информации, DLP-системы.

Objective. The aim of the article is the outsourcing analysis of information technologies related to a commercial enterprise information security.

Methods. In the course of study the following is used: methods of theoretical generalizing and comparison as well as analysis and synthesis (for the content elaboration in the notion of information security outsourcing).

Results. Based on the study conducted the notion is established on the outsourcing of information security of a commercial enterprise, head components are formulated in functioning of information protection systems, in particular, DLP (Data Loss Prevention) system. Besides, the basic advantages and problems of outsourcing are determined, and selection criteria are established on an outsourcer company that would be responsible for complex measures taking in order to provide information security.

Academic novelty. The conceptual system of the outsourcing of a commercial enterprise information security is specified, the scientific methodical approach to selection criteria on an outsourcer company related to protection of commercial information is improved together with prevention of problems arising due to unauthorized data leakage in order to contribute in strengthening of information security of a commercial enterprise.

Practical importance. The findings obtained shall be utilized for optimization of commercial information protection system as well as improvement of a commercial enterprise's information security. The infrastructure of distribution networks information systems has its specific features like large scale and great territorial separation that may lead to the loss of important data. Thus, for information security provision the necessity is substantiated in attracting outside experts of an outsourcing company.

Key words: information security, outsourcing, systems of information protection, DLP systems.

Рекомендовано до публікації д-ром екон. наук,
проф. Оліфіровим О.В. Дата надходження рукопису 28.09.2012 р.