делі: Монографія. / О.В.Раєвнєва; Харк. нац. екон.ун-т. – Харків: ВД „ІНЖЕК”,2006. – 496с.

11. Ребенок А.В. Управління інвестиційним проектом як інструментом реалізації стратегії підприємства / Ребенок А.В. // Актуальні проблеми економіки. – 2008. – №1. – С.154-159.

12. Смоляк С.А. Критерии оптимального поведения фирмы в условиях неопределенности / Смоляк С.А. // Экономика и математические методы. – 2005. – том 41. – №3. – С.39-53.

13. Сорокіна Л.В. Діагностика і регулювання стрибків економічного розвитку підприємств / Сорокіна Л.В. // Актуальні проблеми економіки. – 2007. – №2. – С.93-100.

14. Сорокіна Л.В. Інформаційні технології як інструмент оптимізації управління збалансованим економічним розвитком підприємства / Сорокіна Л.В. // Актуальні проблеми економіки. – 2007. – № 10. — С.189-197.

15. Сорокіна Л.В. Роль актуальних пропорцій в управлінні безпечним розвитком підприємства / Сорокіна Л.В. // Актуальні проблеми економіки.– 2007.– №1. – С.82-90.

16. Статистичний щорічник Донецької області за 2007 рік. / Статистичний збірник. – Донецьк: Державний комітет статистики України, головне управління статистики в Донецькій області, 2008. – 459 с.

17. Трифилова А.А. Оценка эффективности инновационного развития предприятия. / А.А.Трифилова. – М.: Финансы и статистика, 2005. – 304с.

18. Ульяницька О.В. Вплив інвестиційної активності на розвиток інноваційних проектів / Ульяницька О.В. // Актуальні проблеми економіки.– 2008.– №2.– С.36-41.

19. Філіпенко А.С. Глобальні форми економічного розвитку: історія і сучасність. / А.С.Філіпенко. – К.: Знання, 2007. – 670с.

20. Хазан М.М. Организационно-экономический механизм развития в системе управления предприятием / Хазан М.М. // Проблемы теории и практики управления. – 2006. – №2. – С.96-103.

21. Шандова Н.В. Розробка механізму управління стійким розвитком підприємств машинобудування / Шандова Н.В. // Актуальні проблеми економіки. – 2007. – №2. – С.101-105.

Статья поступила в редакцию 19.11.2008

І.О. ДЕЙНЕГА, *к.е.н.,*
М.С. АНДРОЩУК,
Рівненський інститут слов’янознавства

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ: ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ

Інформація, що стосується особливостей функціонування окремого підприємства, забезпечує формування його конкурентних переваг на окремому ринку. Зокрема, це інформація, яка стосується особливостей технологічного процесу, формування витрат, стратегії та тактики поведінки на ринку підприємства, тобто відомості, які згідно з діючим законодавством України відносяться до таємних або конфіденційних (із обмеженим доступом). З іншого боку, отримання таких відомостей про підприємство іншими ринковими контрагентами – його конкурентами, сприятиме послабленню конкурентних позицій визначеного підприємства на конкретному ринку. Ситуація ускладнюється нестабільною макроекономічною ситуацією в Україні, криміналізацією суспільства, підвищенням рівня безробіття, низьким рівнем платоспроможності населення тощо. Тому кожний господарюючий в конкурентному середовищі суб’єкт для підтримання конкурентноздатності повинен забезпечувати захист важливої інформації, стосовно власної ви-

робничої чи господарської діяльності. Вирішити ж проблему захисту інформації можна за рахунок формування систем її захисту.

Практичний досвід існування таких систем на вітчизняних підприємствах визначається десятиріччями існування планово-адміністративної економіки та ґрунтується на побудові служб безпеки на цих підприємствах під егідою держави. Проте науково-методичне забезпечення по створенню систем захисту інформації на підприємствах усіх форм власності не залежно від масштабів їх діяльності (особливо малих) поки що є недостатньо розробленим. При цьому виникає ряд питань, найменш дослідженими з яких є економічні, зокрема пов'язані з економічним тлумаченням самого об'єкту захисту та його характеристик – інформації, а також визначення оптимального співвідношення між витратами на захист інформації та можливими втратами від її витоку.

Таким чином, формування ефективної системи захисту інформації на підприємстві вимагає дослідження та розв'язання значної кількості організаційних, технічних, правових і, особливо, економічних проблем.

Вирішенню проблем захисту інформації присвячена значна кількість наукових і навчально-методичних праць. У більшості з них приділена значна увага технічним і організаційним питанням забезпечення захисту інформації [4, 5, 9, 12-16], проте економічні аспекти формування систем захисту інформації на підприємствах різних форм власності чи взагалі не розглядаються [13,14], чи мають дещо поверхневий характер [4, 5, 9-12, 15-16].

При формуванні економічно доцільних систем захисту інформації на підприємствах в першу чергу необхідно враховувати корисність (цінність) інформації. При вирішенні цього завдання виникають питання, у трактуванні яких науковці й досі не одностайні. Зокрема, це ідентифікація факторів, які впливають на корисність (цінність) інформації, формування підходів до оцінювання корисності (цінності) саме економічної інформації на противагу фізичній та іншим її видам, обґрунтування відмінностей між поняттями "корисність" та "цінність" інформації тощо [1, 2, 6-8].

З початку 60-х років XX століття в роботах вчених прослідковується намагання відійти від виключно кількісного, статистичного оцінювання інформації, проте деякі аспекти оцінювання корисності інформації, зокрема економічний, залишаються або малодослідженими, або не достатньо обґрунтованими, що перешкоджає розробці економічно доцільних систем захисту інформації [1, 2, 6-8].

Метою публікації є розробка науково-методичних та практичних рекомендацій щодо удосконалення системи правових, технічних та організаційних положень захисту інформації на підприємствах різних форм власності та масштабів діяльності в контексті економічної доцільності.

В складних економічних умовах господарювання сучасних українських підприємств, які викликані спадом виробництва та фінансовими труднощами, а також відсутністю їх підтримки зі сторони держави, важливою умовою успішної реалізації власної місії підприємства є створення надійної системи захисту інформації, що забезпечує збереження та розвиток конкурентних переваг підприємства на основі використання його інформаційних ресурсів.

Однак, як показує практика, на більшості вітчизняних підприємствах й досі не сформована "культура захисту інформації", тобто до виникнення критичної ситуації, що спричинена витоком важливої конфіденційної інформації, підприємець або відповідальний менеджер вважає, що діяльність його організаційної структури нікого не цікавить, або що шпигунство – це явище несправжнє, суто літературне. Слід зазначити, що в умовах, коли на ринку присутній більше, ніж один виробник (продавець) певного товару, між ними найчастіше виникає конкурентна боротьба, яка в умовах нерозвитого ринку нерідко є недобросовісною, а одним із методів недобросовісної конкуренції є промислове шпигунство, поява якого обумовлена розвитком ринкової системи господарювання,

розпадом системи жорсткого контролю за виробництвом спеціальної техніки та ввезенням її в країну по офіційних і неофіційних каналах.

Неврегульованість чинного законодавства в сфері захисту інформації теж деякою мірою перешкоджає формуванню на вітчизняних підприємствах ефективних систем захисту інформації. Хоча на Україні існує більше тридцяти законів та нормативних документів у сфері захисту інформації, вони не завжди сприяють створенню передумов ефективного захисту інформації на підприємствах. Зокрема, мова йде про існування різного роду доповнень і уточнень до основних законодавчих актів, які найчастіше послаблюють правові можливості підприємств з точки зору захисту інформації.

Крім того, на деяких підприємствах не має достатньої кількості вільних обігових коштів, які б могли бути направлені на забезпечення захисту інформації. Статистичні дані свідчать про те, що більшість підприємств області різних видів економічної діяльності не мають фінансових можливостей для забезпечення не лише формування повноцінних систем захисту інформації, а й для реалізації першочергових потреб заходів її підтримання .

Хоча захист інформації є важливим атрибутом існування підприємства, його організовування не зможе вирішити всі його проблеми. Необхідно пам'ятати про те, що найважливішим напрямком діяльності більшості підприємства є його основна діяльність, направлена на створення конкретного продукту. Захист інформації лише створює передумови для успішної діяльності підприємства в умовах конкурентного середовища, тому основною метою системи захисту інформації є забезпечення умов для здійснення ефективної діяльності підприємства і всіх його підрозділів.

Для збереження інформації на підприємствах використовуються певні захисні методи (організаційний, технічний, правовий). При цьому система захисту інформації повинна бути адаптована до специфіки зовнішнього середовища підприємства та його внутрішніх можливостей. Саме тому на кожному окремому підприємстві методи захисту інформації можуть бути різні за масштабами і формою. Кількісний і якісний склад способів і прийомів захисту інформації залежить:

від специфіки виробничої діяльності (найбільше потребують захисту інформації підприємства, котрі функціонують в умовах інтенсивної конкуренції, діяльність яких напряму залежить від якості (своєчасності, достовірності тощо) інформації (банківські організації, консалтингові фірми, засоби масової інформації тощо));

від виробничих, фінансових й інших можливостей підприємства;

від кількості таємних і конфіденційних відомостей, які використовуються конкретним підприємством і потребують захисту, а також корисності (цінності) інформації.

Аналіз базових теорій по визначенню цінності інформації виявив переважно теоретичний характер вирішення цієї проблеми. Критерії та показники, що пропонуються в якості оцінювання цінності (корисності) інформації, в більшості теорій важко піддаються кількісному підрахунку через абстрактну чи значну суб'єктивну природу їх формування [1, 2, 6-8].

Безперечно, на корисність інформації будуть впливати й апріорний запас відомостей споживача інформації, й послідовність дій, в якій він буде вирішувати конкретне завдання, та багато інших факторів, проте основним при оцінюванні корисності економічної інформації залишається визначення матеріального (фінансового чи іншого) ефекту від її використання. Недарма ще Л.Бріллюен зазначав, що економічні параметри предметів, створених працею людини, в тому числі інформаційних видань, більш точно відображають їх цінність, ніж фізичні характеристики, оскільки за допомогою економічних показників привносяться оцінки людини, що відображають корисність предмета для споживача [6, с.256], хоча визначення впливу інформації на отриманий у матеріальному виробництві ефект пов'язане з рядом ускладнень.

На нашу думку, доцільно здійснюва-

ти оцінювання корисності інформації в залежності від об'єкту, що використовує її потенціал. Так, корисність інформації для підприємства буде залежати від корисності інформації всіх споживачів інформації, а також узгодженості, координованості, швидкості руху інформаційних потоків на підприємстві тощо.

Таким чином, узагальнення результатів проведеного дослідження способів оцінювання цінності інформації, дозволяє виділити наступні фактори, що визначають та забезпечують корисність інформації для підприємства:

рівень професійної підготовки чи апріорний запас відомостей, або тезаурус споживача інформації;

відповідність інформації системі показників якості інформації [3, с.343-344];

важливість завдання, для вирішення якого інформація буде використовуватися, що впливатиме безпосередньо на величину очікуваного ефекту від її використання.

При забезпеченні ефективного захисту інформації на підприємствах необхідно дотримуватися певних організаційно-економічних принципів, основними з яких є економічна доцільність, активність, впевненість, безперервність, різноманітність, комплексність (цілісність) захисту інформації; принципи динаміки та законності.

Формування системи захисту інформації повинно в першу чергу здійснюватися за принципом економічної доцільності, адже як і халатне відношення до зберігання (захисту) інформації, так і надмірне її засекречування в однаковій мірі можуть викликати втрату частини прибутку чи призвести до непоправних економічних втрат. Формуючи перелік відомостей, які складають комерційну таємницю, не слід також забувати і про те, що існує й законодавчо обумовлена відповідальність за навмисне приховування інформації.

Для того, щоб забезпечити економічну доцільність захисту інформації, необхідно, щоб можливі втрати від витоку інформації повинні бути дещо більшими витрат на її захист. Критичним рівнем витрат на захист інформації, вищим за який вони бути не можуть, буде величина ймовірних втрат від витоку інформації. Оптимізація досягається при мінімізації витрат на захист інформації, тобто, чим нижчий рівень даних витрат, тим економічно доцільнішою є система захисту інформації. Однак, нижня межа витрат, звісно, не повинна бути нульовою.

Економічна доцільність захисту інформації буде підвищуватися за рахунок скорочення витрат на захист інформації при одночасному підвищенні (підтримці) загального рівня якості системи її захисту, тому встановлення можливих втрат від витоку певної інформації є задачею більше економічною, ніж організаційною. Адже від розрахованої величини можливих втрат від витоку інформації буде залежати величина коштів, що можуть будуть витрачені на її захист, а, отже, і кількісний та якісний зміст складових системи захисту інформації на підприємстві.

Ця залежність може бути використана також і для перевірки відповідності вже діючої системи захисту інформації на підприємстві вимозі економічної доцільності. При цьому вартісне значення витрат на захист визначається на основі кошторису (кількісно це сума витрат на проведення всіх захисних заходів).

Величина витрат на захист певної інформації повинна періодично переглядатися. Періодичність формування витрат на захист певної інформації буде залежати, в першу чергу, від інтенсивності її старіння, тобто проміжку часу, на протязі якого дана інформації може перейти з розряду особливо важливої до важливої та, врешті-решт, корисної або несуттєвої.

На рис. 1 наведена структура причин витоку інформації, де визначено, що безпека економічної діяльності й ефективність захисту інформації будь-якої комерційної структури залежить в першу чергу від кваліфікації її співробітників, їх морально-етичних якостей, якості роботи з персоналом у сфері захисту інформації. Відповідно, найбільш важливою є задача об'єктивної вартісної оцінки можливих втрат від витоку інформації. Спеціалісти всіх служб підприємства повинні навчитися правильно оцінювати реальні та можливі втрати

підприємства внаслідок витоку інформації.

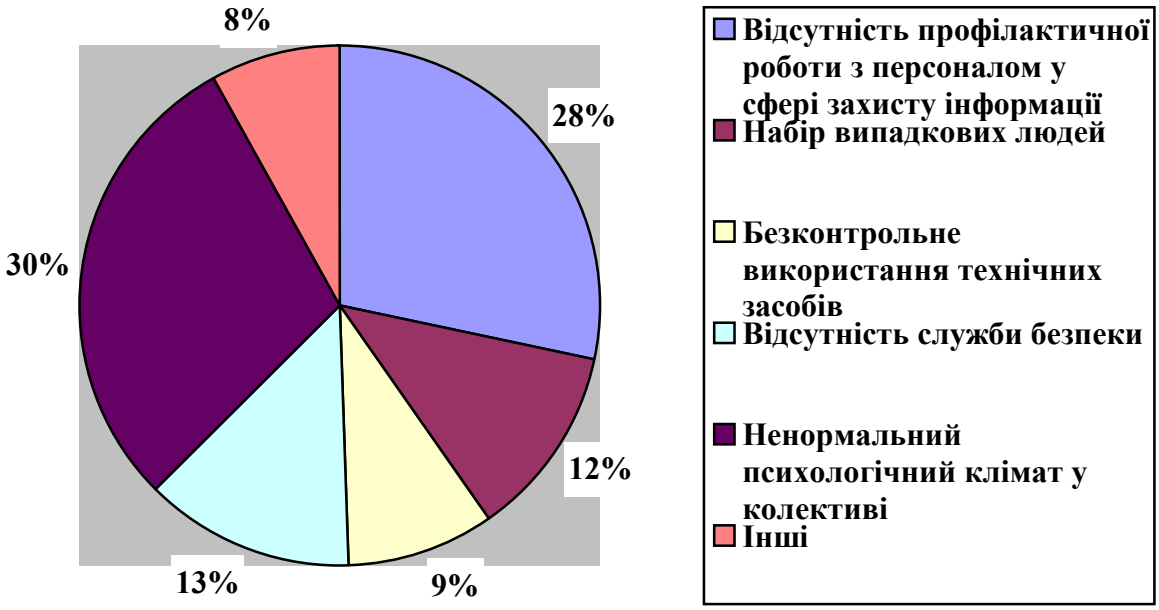

Рис. 1. Структура причин витоку інформації на підприємстві

Джерело: опрацювання власне на основі даних опитування керівників автотранспортних підприємств, м.Рівне

Втрати від витоку інформації можуть бути спричинені такими обставинами: втрата пріоритету в освоєних областях науково-технічного прогресу, зростання витрат на переорієнтацію діяльності дослідницьких підрозділів; втрата довіри споживача до якості продукції; виникнення чи створення конкурентами труднощів із закупівлею сировини, технологій, обладнання й інших компонентів, необхідних для здійснення нормальної виробничої діяльності; ускладнення відносин з партнерами, зрив вигідних контрактів і договірних зобов'язань; ріст витрат на створення нової ринкової стратегії, зміну плану проведення маркетингових досліджень тощо. Таким чином, ці втрати можуть бути:

прямими економічними (вартісними), тобто відразу вираженими в певній грошовій сумі;

у вигляді втрати підприємством вигідного становища на ринку;

у вигляді ускладнень відносин із діловими партнерами, клієнтами.

У будь-якому випадку втрати від витоку важливої конфіденційної інформації будуть економічними. Лише тривалість їх трансформування може бути різною. Зокрема, ускладнення відносин із постачальниками може сприяти тому, що підприємство втратить доступ до дешевих сировинних ресурсів, що, в свою чергу, вплине на зростання прямих виробничих витрат і собівартості продукту. Зростання собівартості продукту призведе або до зростання ціни продукту (можливість втрати ринкової частки), або до зниження його рентабельності. І в тому, і в іншому випадку підприємство втратить частину прибутку.

Інший приклад – втрата довіри споживачів до якості продукту. Це може призвести до зниження обсягів та виручки від його реалізації та, відповідно, до втрати підприємством частини прибутку. Опосередковано втрати від витоку інформації можуть бути оцінені через корисність останньої.

Точний вартісний розрахунок втрат від витоку інформації досить важкий, а часом і не можливий через відсутність якісних даних, а також через постійну динамічну зміну споживної вартості інформації, що потребує захисту. Тому в ряді випадків досить обмежитися зведеною експертною оцінкою. Експертами можуть виступати керівник підприємства, начальник служби

безпеки, а також керівники відділів і служб підприємства, що мають доступ до важливої інформації. Вимога до підбору експертів одна: експерт повинен бути достатньо знайомий з проблемою і мати про неї власну думку. Звісно, експерт не повинен бути зацікавлений в отриманні певного результату.

Надійність отриманих оцінок значною мірою залежить від правильного підбору експертів, їх кваліфікації, ерудиції, інформованості в питаннях, які досліджуються. Знання експертами предмету дослідження та їх аналітичні здібності перевіряються шляхом тестування. Точність результату залежить від статистичної обробки результатів дослідження. Створюється робоча група, яка розробляє комплекс задач, що висуваються перед експертами (дерево цілей). Використовуються методи логічного обґрунтування, будуються гіпотези стосовно результатів дослідження. На цій основі розробляється анкета/опитувальник. Число питань не повинно бути надмірним, адже чисельність експертів знаходиться в пропорційній залежності від нього.

Крім принципу економічної доцільності при формуванні раціональних систем захисту інформації на підприємстві, необхідно дотримуватися також і інших принципів. Зокрема, принципу активності захисту інформації, який виражається в цілеспрямованому нав'язуванні комерційній розвідці неправдивої інформації про об'єкт її розвідувальних наполягань, у відповідності з задумом захисту. Безперервність захисту інформації передбачає організацію захисту об'єкта на всіх стадіях його життєвого циклу збір-обробка–споживання–знищення, а принцип різноманітності захисту інформації – виключення шаблонів, повторів у виборі об'єкту прикриття і шляхів реалізації змісту захисту, в тому числі з використанням типових рішень. Суть принципу законності полягає в тому, що побудова системи захисту інформації повинна здійснюватись із дотриманням всіх існуючих на даному етапі розвитку суспільних відносин законів та нормативних документів в сфері захисту інформації.

Важливим принципом організовування захисту інформації на підприємстві є принцип динаміки. Його суть полягає в тому, що комплекс заходів по захисту інформації повинен періодично змінюватися (переглядатися). Це пов'язано, насамперед, із безперервним розвитком способів і засобів економічного шпигунства. Основним критерієм, що визначає термін дії даного комплексу, є наступна умова: "Комплекс заходів по захисту інформації повинен діяти рівно стільки часу, скільки необхідно для того, щоб розробити комплекс заходів по неправовому збору даної інформації" [9, с. 144]. Крім того, на підприємстві повинні діяти всі захисні методи одночасно і з однаковою інтенсивністю. Це забезпечить виконання принципу комплексності (цілісності). Оскільки ефективність дії всієї системи буде визначатись якістю найгіршої її складової. Цілісність дії системи захисту інформації буде також обумовлюватись: єдиною метою її функціонування, налагодженістю та узгодженістю інформаційних зв'язків між її елементами, ієрархічністю побудови підсистеми управління системою захисту інформації. Комплексність дії системи захисту інформації досягається за допомогою створення та координування ефективної роботи власної служби безпеки.

Система захисту інформації має лише відносно самостійне значення, оскільки в процесі свого функціонування вона обов'язково вступає у складні зв'язки з усіма іншими системами та підсистемами підприємства, його зовнішнім середовищем. Тому основною її метою є забезпечення нормального й ефективного функціонування системи вищого рівня управління, в яку вона вбудована і для якої створена, а саме системи управління підприємством.

Проблемі захисту інформації в сучасних умовах, які склалися, будь-яке підприємство повинно приділяти якнайбільшу увагу, оскільки це є одним із важливих аспектів, що забезпечує його ефективну роботу в умовах вільного конкурентного ринку. Позитивні результати в конкурентній боротьбі можуть бути і не отримані, якщо

важлива конфіденційна інформація про особливості товару підприємства, зокрема його якісні параметри, терміни і методи виведення такого товару на ринок тощо стане відомою економічним суперникам, так як це дозволить їм прийняти відповідні контрзаходи. Перевага за часом як фактор конкурентної боротьби може бути реалізована лише при забезпеченні ефективного захисту конфіденційної та таємної інформації підприємства. З іншого боку, надмірні (економічно не виправдані) витрати на захист інформації підприємства можуть призвести до необґрунтованого збільшення загальних витрат підприємства, зменшення економічних результатів його діяльності. Відповідно, на теперішньому етапі розвитку ринкових відносин керівники підприємств та окремі підприємці повинні переосмислити підходи до забезпечення захисту інформації з точки зору економічної доцільності останнього і чітко усвідомити його необхідність.

Література

1. Баззел Р., Кокс Д., Браун Р. Информация и риск в маркетинге/ Пер. с англ. под ред. М.Р. Ефимовой. – М.: Финстатинформ, 1993. – 96 с.

2. Бройдо В.Л. Достоверность экономической информации в АСУ. – Л: Изд-во Ленинградского ун-та, 1984. – 200 с.

3. Дейнега И.А., Патора Р. Информационное обеспечение рационального использования ресурсов предприятий // Инновационное развитие топливно-энергетического комплекса: проблемы и возможности / Под общ. ред. Г.К. Вороновского, И.В. Недина. – К.: Знания Украины, 2004. – С.343-346.

4. Духов В.Е. Экономическая разведка и безопасность бизнеса.-К:ИМСО МО Украины, НВФ «Студцентр», 1997. – 175с.

5. Зубик В.Б., Седегов Р.С., Абдула А. Экономическая безопасность предприятия (фирмы). – Мн.: Выш. шк., 1998. – 391с.

6. Злочевський С.Е., Козенко А.В., Косолапов В.В., Половинчик А.Н. Информация в научных исследованиях. – К.: Наукова думка, 1969. – 288 с.

7. Мамиконов А.Г. Принятие решений и информация. – М.: Наука. – 1983. – 184 с.

8. Мамиконов А.Г. Управление и информация. – М.: Наука, 1975. – 183 с.

9. Организация и современные методы защиты информации / Под ред. С.А.Диева, А.Г.Шаваева – М: Концерн «Банк. Дел. Центр». – 1998.– 472 с.

10. Постоловський Р.М, Дейнега І.О., Дейнега О.В. та ін. Методи збору, обробки та захист комерційної інформації: – Рівне: Рівненський інститут слов'янознавства КіСУ, 2002. – 305 с.

11. Чернявский А.А. Промышленный шпионаж и безопасность предпринимательства. – К: МЗУУП. – 1994. – 64с.

12. Шиферский А.А. Защита информации: проблемы теории и практики. – М: Юристь. – 1996. – 112с.

13. Андрианов В.И., Соколов А.В. «Шпионские штучки» и устройства для защиты информации.- СПб.:Лань. – 1996. – 266с.

14. Андрианов В.И., Соколов А.В. «Шпионские штучки-2» или как сберечь свои секреты.- СПб.: Полигон. – 1997. – 272с.

15. Ярочкин В. Коммерческая информация фирмы. – М.: Ось-89. – 1997. – 79 с.

16. Ярочкин В. Система безопасности фирмы. – М.: Ось-89. – 1998. – 192с.

Статья поступила в редакцию 19.11.2008