УДК 336.763.2

І. П. Шульга,
к. е. н., доцент, доцент кафедри фінансів та кредиту,
Східноєвропейський університет економіки і менеджменту

РОЛЬ ІНСАЙДЕРСЬКОЇ ІНФОРМАЦІЇ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ АКЦІОНЕРНИХ ТОВАРИСТВ

Досліджено поняття "інсайдер" в українському законодавстві та наведено характеристику осіб, що до них належать. Встановлено види інсайдерів у залежності від причин, що їх спонукають до розголошення інсайдерської інформації. Проаналізовано структуру суб'єктів витоку інсайдерської інформації про діяльність акціонерного товариства та факторів, які їх спричинили.

A concept "insider" is investigational in the Ukrainian legislation and description over of persons is brought, that to them belong. The types of insiders are set, depending on reasons, that they are induced to the disclosure of insider`s information. The structure of subjects of source of insider`s information is analysed about activity of joint-stock company and factors which entailed them.

Ключові слова: інсайдер, інформація, акціонерне товариство, працівник, загрози, способи захисту від загроз.
Key words: insider, information, joint-stock company, worker, threats, methods of protecting from threats.

ВСТУП

Розвиток фондового ринку України потребує прийняття невідкладних заходів щодо недопущення маніпуляцій ринком цінних паперів, нечесної торгової практики і порушення етики професійної діяльності на фондовому ринку. Окремої уваги потребує питання використанні інсайдерської інформації про акціонерні товариства, особливо з приведенням їх діяльності у відповідність із законом "Про акціонерні товариства", який вимагає чіткого дотримання окремих положень щодо кількості акціонерів, форми випуску акцій, структури управління товариством тощо. Використання інсайдерської інформації саме у цей перехідний період підвищує загрози рейдерських захоплень з метою зміни власників та недружнього поглинання.

Прийняті правила проведення операцій з інсайдерами є частиною кодексу корпоративної етики і однією з практик корпоративного управління, які повинні використовувати всі акціонерні товариства, що хочуть отримати статус публічної компанії, що й підтверджує актуальність теми дослідження.

Проблемам захисту акціонерних товариств від витоку інформації та її використання зацікавленими особами для отримання власної вигоди при здійснення операцій з акціями даного емітента присвячені праці зарубіжних та вітчизняних науковців та практиків Ткачука Т.С. [3], Скиби Б.Ю., Курбатова Б.А. [4], Глушкова В.О., Коваленка П.М. [5], Кавуна С.В., Носова В.В., Манжая О.В. [6] та інших.

ПОСТАНОВКА ЗАВДАННЯ

Метою дослідження є встановлення ролі інсайдерської інформації у забезпеченні економічної безпеки акціонерних товариств України. Основними методами досягнення поставленої мети є систематизація — при узагальненні видів інсайдерів, їх загроз та способів захисту; вертикального налізу — при визначенні структури суб'єктів витоку інсайдерської інформації про діяльність акціонерного товариства та факторів, які їх спричинили.

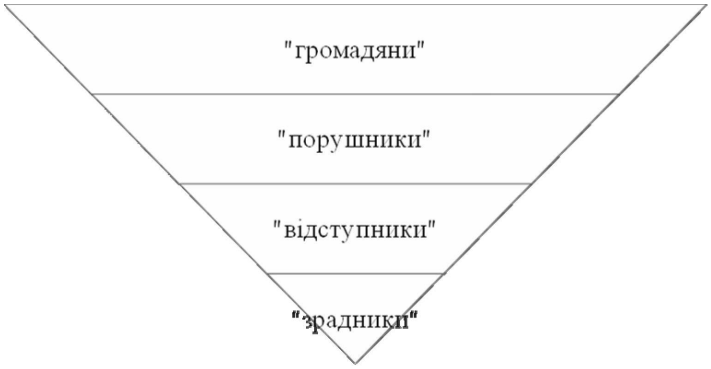

Рис. 1. Класифікація інсайдерів згідно досліджень IDC

РЕЗУЛЬТАТИ

На сьогоднішній день існує все більше можливостей отримання інформації, в тому числі й інформації з обмеженим доступом, тобто такої інформації, витік якої може завдати шкоди її власнику. З'являється все більше загроз витоку даних, а з розвитком новітніх технологій способи їх отримання постійно вдосконалюються. Отже, існує і багато засобів, що повинні забезпечувати захист інформації з обмеженим доступом. Крім технічних засобів захисту, є безліч інструкцій, правил, які регламентують поводження із такою інформацією, а також є ціла низка нормативних актів, з яких ці інструкції випливають. Захоплюючись технічними можливостями витоку та захисту від витоку інформації, багато керівників забувають, що загроза витоку інформації може бути пов'язана з їхнім власним персоналом, тобто з інсайдерами.

Термін інсайдер походить від англійського "inside" — в середині — і зазвичай означає коло осіб (і юридичних, і фізичних), які мають доступ до закритої інформації. Разом з тим, навіть у нормативно-правових актах України зустрічаються різні визначення поняття "інсайдер".

Так, у Законі України "Про цінні папери та фондовий ринок" [1] поняття "інсайдери" регламентується як особи, які володіють інсайдерською інформацією у зв'язку з тим, що вони є:

1) власниками голосуючих акцій емітента або часток (паїв) у статутному капіталі емітента;

2) посадовими особами емітента;

3) особами, які мають доступ до інсайдерської інформації у зв'язку з виконанням трудових (службових) обов'язків або договірних зобов'язань незалежно від відносин з емітентом, зокрема:

— юридичними особами, які перебувають з емітентом у договірних відносинах або прямо чи опосередковано у відносинах контролю;

— фізичними особами, які перебувають з емітентом, юридичними чи фізичними особами, пов'язаними з емітентом договірними відносинами або відносинами контролю, у трудових чи договірних відносинах або прямо чи опосередковано у відносинах контролю;

— державними службовцями.

"Концепція запобігання маніпулюванню ринком цінних паперів, нечесній торговій практиці і порушенню етики професійної діяльності на фондовому ринку" зазначає, що "інсайдер" — це "особа, яка має доступ до інсайдерської інформації завдяки тому, що вона є:

1) власником понад 10 % голосуючих акцій емітента або часток (паїв) у статутному фонді, які мають контроль над емітентом;

2) посадовою особою емітента;

3) особою, яка мала доступ до інсайдерської інформації у зв'язку з виконанням трудових (службових) обов'язків або договірних зобов'язань незалежно від наявності прямих відносин з емітентом, зокрема:

— юридичною особою, які перебувають з емітентом у договірних відносинах або прямо чи опосередковано у відносинах контролю;

— фізичною особою, яка перебуває з емітентом, юридичною чи фізичною особою, пов'язаними з емітентом договірними відносинами або відносинами контролю, у трудових чи договірних відносинах, або прямо чи опосередковано у відносинах контролю;

— державним службовцем; фізичною або юридичною особою, яка перебуває у трудових чи договірних відносинах, або прямо чи опосередковано у відносинах контролю, з особами, що мають намір придбати цінні папери емітента" [2].

Однією з перших крок в напрямі класифікації зробила міжнародна науково-дослідна компанія IDC, що представила свій погляд на проблему в 2006 році. За версією IDC, система інсайдерів має чотири рівні: "громадяни", "порушники", "відступники", "зрадники" (рис. 1).

Верхній рівень складають "громадяни" — лояльні службовці, які дуже рідко (якщо взагалі коли-небудь) порушують корпоративну політику і в основному не є загрозою безпеці [3].

На другому рівні знаходяться "порушники", що складають велику частину усіх співробітників підприємства. Ці співробітники дозволяють собі невеликі фамільярності, працюють з персональною веб-поштою, грають в комп'ютерні ігри і здійснюють онлайнові покупки. Представники даного рівня порушників створюють загрозу інформаційній безпеці, але ці інциденти є випадковими і ненавмисними.

На наступному рівні знаходяться "відступники" — працівники, які велику частину робочого часу роблять те, що вони робити не повинні. Ці службовці зловживають своїми привілеями по доступу до Інтернету. Більш того, такі співробітники можуть посилати конфіденційну інформацію компанії зовнішнім адресатам, зацікавленим в ній. Таким чином, "відступники" представляють серйозну загрозу безпеці.

На нижньому рівні знаходяться "зрадники" — це службовці, які умисно і регулярно піддають конфіденційну інформацію компанії небезпеці (зазвичай за фінансову винагороду від зацікавленої сторони). Такі співробітники представляють реальну загрозу, але їх найскладніше зловити [4].

Більш широка класифікація представлена російською компанією Info Watch [4]. Фахівці компанії фокусують увагу винятково на захисті даних від витоку, спотворення і знищення, тому їх погляди відрізняються більшою глибиною аналізу.

"Недбалий інсайдер" — цей вид інсайдерів є найчисленнішим серед інших. Зазвичай ним є рядовий внутрішній співробітник, який порушив вимоги про конфіденційність інформації через свою неуважність. Таким чином, у діях даного виду інсайдера не можна знайти ні користі, ні наміру, ні будь-яких цілей — він порушує вимоги про конфіденційність інформації невмотивовано.

Дане порушення відбувається внаслідок незловмисного порушення працівником правил зберігання конфіденційної інформації. При цьому мотиви таких інсайдерів можуть бути найкращими — "виконати п'ятирічку за чотири роки". Іншими словами, такі порушники можуть виносити інформацію з офісу компанії для того, щоб працювати з нею вдома або під час відрядження. Надалі носій інформації губиться або до нього отримують доступ члени сім'ї інсайдера. У результаті збитки від витоку інформації від цього нітрохи не менше, ніж у випадку промислових шпигунів.

Даний тип інсайдера буде діяти відповідно до інструкцій, а саме — почне задавати питання системному адміністратору або колегам про причини неможливості копіювання інформації та отримає роз'яснення про те, що виносити інформацію за межі офісу суворо забороняється. Для захисту від таких інсайдерів достатньо простих технічних засобів щодо запобігання каналів витоку: централізація роботи пристроїв управління введенням / виведенням інформації і контентна фільтрація вихідного трафіку.

"Інсайдер, яким маніпулюють" підпадає під дію так званої "соціальної інженерії", яка, впливаючи на нього, спонукає до знехтування деякими заплутаними і "непотрібними" інструкціями, які забороняють будь-яке розкриття конфіденційної інформації заради "кращого" компанії.

Основними методами "соціальної інженерії" є:

Претекстінг — це дія, відпрацьована за наперед складеним сценарієм (претекстом). У результаті людина повинна видати певну інформацію або зробити певну дію. Цей вид атак застосовується зазвичай по телефону. Частіше ця техніка включає більше, ніж просто оману, і вимагає яких-небудь попередніх досліджень (наприклад, персоналізації: дата народження, сума останнього рахунку тощо) з тим, щоб забезпечити довіру людини.

Фішинг — техніка, направлена на шахрайське отримання конфіденційної інформації. Зазвичай зловмисник посилає цілі e-mail, підроблені під офіційний лист, від банку або платіжної системи, що вимагає "перевірки" певної інформації або здійснення певних дій.

Троянський кінь — ця техніка експлуатує цікавість, або жадібність людини. Зловмисник відправляє e-mail, що містить досить цікаву для людини інформацію, наприклад свіжий компромат на співробітника. Така техніка залишається ефективною, поки користувачі сліпо клікатимуть по будь-яких закладках.

Дорожнє яблуко — цей метод атаки є адаптацією троянського коня і полягає у використанні фізичних носіїв. Зловмисник може підкинути інфікований CD або флеш, в місці, де носій може бути легко знайдений. Носій підробляється під офіційний і супроводжується підписом, покликаним викликати цікавість.

Кві про кво — зловмисник може подзвонити по випадковому номеру в компанію і представитися співробітником відділу технічної підтримки, що опитує, чи є які-небудь технічні проблеми. У випадку, якщо вони є, в процесі їх "вирішення" людина вводить команди, які дозволяють зловмисникові запустити шкідливе програмне забезпечення [4].

Зловмисник отримує інформацію, наприклад, шляхом збору персональних даних про службовців об'єкта атаки, за допомогою звичайного телефонного дзвінка або шляхом проникнення в організацію під виглядом її службовця.

Найкращий захист від таких інсайдерів — це створення такої ситуації, в якій вони не могли б порушити регламенти зберігання і поширення інформації, натрапивши на технічне блокування подібного роду спроб.

Усі наступні групи інсайдерів — скривджені, нелояльні, ті, що хотіли підзаробити, і заслані — відносяться до зловмисних інсайдерів, які діють переконливо й усвідомлено, знаючи про негативні наслідки своєї діяльності. Їх відмінність залежить від мотивів ворожих дій, здійснюваних ними.

"Скривджений інсайдер" — це співробітник компанії, що розкриває конфіденційну інформацію для того, щоб здійснити помсту компанії з особистих мотивів. А ці мотиви можуть бути найрізноманітнішими — від образи на директора компанії, який у черговий раз не підвищив співробітника на посаді, до елементарної відсутності моральної мотивації працювати на краще компанії.

Скривдженого інсайдера можна виявити за наступними двома ознаками:

1) у його наміри не входить залишити компанію;

2) його метою є нанесення шкоди, а не викрадення інформації як такої.

Таким чином, дані інсайдери діють так, щоб керівництво компанії не здогадалося про те, що інформація була викрадена саме ним, тому натрапивши на технічний бар'єр, що перешкоджає викрадення інформації, такий інсайдер, як правило, направить свою руйнівну силу на будь-який інший об'єкт, наприклад, на викрадення майна компанії або на фальсифікацію чи знищення наявної інформації. Важливим є й те, що ображений інсайдер при викраденні інформації виходить з власних міркувань про її важливість і значущість для компанії. У визначенні адресата, якому слід передати викрадену інформацію, скривджені інсайдери найчастіше зупиняють свій вибір на пресі або будь-яких тіньових структурах. При цьому оголошення і подальший шантаж — головна мета, яка ставилася ними.

"Нелояльний інсайдер" — це співробітник, що вирішив звільнитися або ж відкрити власний бізнес. Як правило, саме на таких людей падає перша підозра керівників компанії в разі викрадення інформації. Адже часто так і виходить, що звільняючись, співробітник з комерційного відділу прихоплює з собою копію бази клієнтів, а співробітник страхової компанії — копію бази застрахованих осіб. Тимчасові стажисти також можуть бути віднесені до даної категорії, оскільки останнім часом спостерігається збільшення розкрадання інформації з офісів високотехнологічних компаній Сполучених Штатів і Європи стажистами з країн третього світу.

Таблиця 1. Характеристика інсайдерів компанії, загроз та способів захисту від них

	Вид інсайдера	Характеристика інсайдера	Характеристика загрози	Спосіб захисту
Несвідомі порушники	«недбалий інсайдер»	найбільш поширений тип внутрішніх порушників. Його порушення у відношенні конфіденційної інформації мають немотивований характер, не мають конкретних цілей, наміру, користі	втрата інформації, її розголошення	централізація роботи пристроїв управління введенням / виведенням інформації
	«інсайдер, яким маніпулюють»	співробітники, яких обманним шляхом штовхають на порушення встановлених норм. Такі співробітники часто і не підозрюють про те, що їхні дії призводять до втрати конфіденційних даних	ненавмисна передача інсайдерської інформації стороннім особам під впливом «соціальної інженерії»	централізація роботи пристроїв управління введенням / виведенням інформації
Свідомі порушники	«скривджені інсайдери», або саботажники	співробітники, які прагнуть завдати шкоди компанії через особисті причини	розповсюдження інформації у пресі або кримінальних структур, її псування або пошкодження	підвищення ефективності роботи служби економічної безпеки, відділу кадрів та профспілок
	«нелояльні інсайдери»	співробітники, що вирішили змінити місце роботи, або акціонери, що вирішили відкрити власний бізнес	заволодіння інформацією з/або без зовнішнього розповсюдження, шантаж керівництва	
	«інсайдери, що вирішили підзаробити»	співробітники, які вирішили продати інсайдерську інформацію замовнику	передача інформації конкурентам, особам, що готують поглинання чи захоплення	підвищення ефективності роботи служби економічної безпеки
	«впроваджені інсайдери»	співробітники, які влаштувались на роботу в компанію з метою здобуття та передачі інформації замовнику		

Складено особисто автором.

Головною особливістю є те, що загроза даних інсайдерів є ненаправленою, тобто такі порушники часто не підозрюють про конкретну цінність викраденої ними інформації, а також іноді не мають уявлення про те, як вони збираються використовувати її у подальшому. Імітація виробничої необхідності — улюблений спосіб, що дозволяє скопіювати конфіденційну інформацію даними співробітниками, при цьому їх досить часто помічають за таким заняттям.

Їх головна відмінність від скривджених інсайдерів полягає в тому, що нелояльні співробітники не приховують сам факт викрадення інформації. Навпаки, у деяких випадках вони навіть відкрито заявляють про це директору компанії, маючи на меті забезпечення більш комфортного звільнення: з наданням компенсацій, рекомендацій і певного роду гарантій. Намагаючись забрати якомога можна більшу кількість конфіденційної інформації, даний тип співробітників являє собою ненаправлену загрозу для компанії. При цьому вони самі часто не підозрюють про те, яку цінність являє собою викрадена ними інформація, а також те, як вони будуть використовувати її у подальшому.

"Інсайдер, що вирішив підзаробити". Проте, ситуація з нелояльними і скривдженими інсайдерами змінюється корінним чином, якщо вони попередньо вийшли на зв'язок з покупцем інформації, передбачуваної до викрадення. Головна відмінність буде полягати в меті: у інсайдерів, що вирішили підзаробити, та "засланих" інсайдерів — це буде прагнення заробити гроші за передачу інформації. У деяких випадках від правильності виконання "роботи" залежатиме їх власне життя і здоров'я. Інсайдер, що вирішив підзаробити, та "засланий" інсайдер не визначають мету викрадення інформації самостійно, це робить за них потенційний замовник. Також, як і у випадку зі скривдженими співробітниками, інсайдер, що вирішив підзаробити, буде прагнути якомога надійніше приховати свої дії від сторонніх спостерігачів (принаймні, поки їм не вдасться викрасти інформацію), однак при цьому цілі скривджених і тих, хто вирішив підзаробити, кардинально різняться.

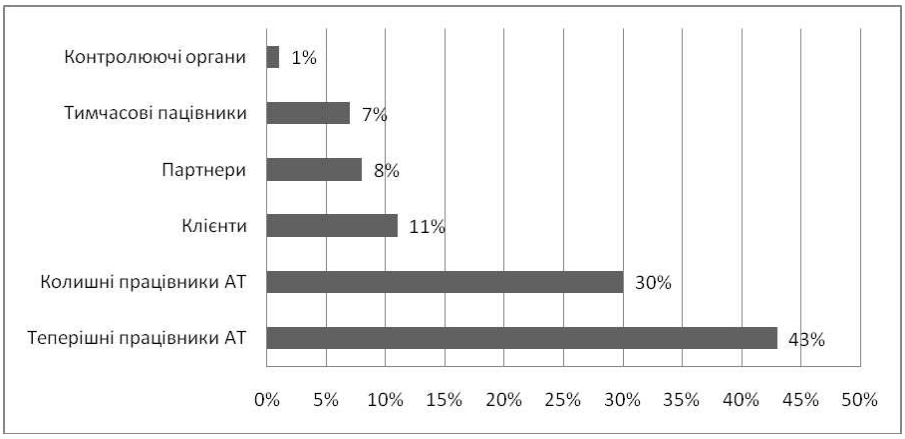

Рис. 2. Структура суб'єктів витоку інсайдерської інформації про діяльність акціонерного товариства

Мотиви інсайдерів, що вирішили підзаробити, можуть різні: від бажання заробити суму, якої бракує їм для довгоочікуваної покупки, до дії з примусу, коли таких співробітників шантажують ті чи інші структури і вони вже не мають іншого вибору, як викрасти конфіденційну інформацію,

Таблиця 2. Фактори розголошення співробітниками інформації [5]

№ п/п	ФАКТОРИ	%
1	Надмірна балакучість співробітників	32
2	Прагнення співробітників заробляти гроші будь-якими способами та за будь-яку ціну	24
3	Відсутність на фірмі служби безпеки	14
4	«Радянські» звички співробітників фірми ділитися один з одним (традиційний обмін досвідом)	12
5	Безконтрольне використання інформаційних систем	10
6	Наявність можливостей виникнення серед співробітників конфліктних ситуацій: відсутність психологічної сумісності, випадковий підбір кадрів, відсутність роботи щодо згуртованості колективу і т.д.	8

тому що в протилежному випадку на кону стоїть їх власне життя чи здоров'я або життя і здоров'я членів їх сім'ї. З цієї причини інсайдер, що вирішив підзаробити, не зупинить своїх спроб у разі технічних бар'єрів, що перешкоджають отриманню інформації. Імітація виробничої необхідності — також досить часто застосовується ними хід. У крайніх випадках такі співробітники можуть піти навіть на підкуп інших співробітників компанії.

"Засланий" інсайдер. Не варто вважати, що такі інсайдери існують тільки в шпигунських трилерах, насправді шпигунство сьогодні використовується не тільки для одержання секретів державного значення, але також і в промисловій сфері. Головна небезпека, що виходить від "засланих" інсайдерів, полягає в тому, що вони забезпечені необхідними технічними навичками, що дозволяють їм подолати всі технічні бар'єри на шляху до отримання конфіденційної інформації.

Виходячи із досліджених загроз діяльності акціонерним товариствам та загроз розповсюдження інсайдерської інформації через працівників товариства, автором було систематизовано основні види інсайдерів, загроз, які вони викликають, та способів захисту від них (табл. 1).

Інсайдерські інциденти відбуваються набагато частіше, ніж зовнішні атаки. Компанії прагнуть не афішувати свої внутрішні проблеми, але авторитетні дослідження все одно віддають пальму першості інсайдерам. Так, згідно дослідженню 2005 E-Crime Watch Survey, проведеному організацією CERT, в ході якого було опитано більше 800 компаній, кожна друга компанія хоч би раз протягом року постраждала від витоку даних (рис. 2).

Аналітики підрахували, що 43 і 30 % інцидентів викликані нинішніми і колишніми співробітниками відповідно, 11% припадають на частину клієнтів компанії, 8 % відбуваються через партнерів і, нарешті, 7 % викликані тимчасовими службовцями (контрактниками, консультантами тощо). Це свідчить про те, що проблема витікання конфіденційної інформації стає на перше місце в списку пріоритетів керівництва компанії [6].

Дані антирейдерського союзу підприємців України свідчать, що:

— 82% загроз реалізується власними співробітниками фірми або за їх прямої чи опосередкованої участі;

— 17% загроз реалізується ззовні підприємства;

— 1% загроз реалізується випадково.

Найпоширеніші фактори розголошення співробітниками інформації з обмеженим доступом наведені у табл. 2.

Як видно з таблиці, розголошення співробітниками інформації з обмеженим доступом найчастіше здійснюється через те, що керівництво компаній не приділяє уваги загрозам витоку інформації, пов'язаним з персоналом, тобто, інсайдерами.

Отже, проаналізувавши загрози конфіденційності даних, які пов'язані з персоналом, можна побачити, що ігнорування цих загроз призводить до серйозних збитків на підприємствах. Мова йде не тільки про фінансові втрати компанії, але й про різке падіння її іміджу у зв'язку з тим, що вона не може захистити власну конфіденційну інформацію.

ВИСНОВКИ

У результаті проведеного дослідження було зроблено наступне:

— досліджено поняття "інсайдер" в українському законодавстві та наведено характеристику осіб, що до них належать;

— систематизовано види інсайдерів у залежності від причин, що їх спонукають до розголошення інсайдерської інформації;

— проаналізовано структуру суб'єктів витоку інсайдерської інформації про діяльність акціонерного товариства та факторів, які їх спричинили;

— встановлено роль інсайдерської інформації у забезпеченні економічної безпеки акціонерних товариств України.

Література:

1. Закон України "Про цінні папери та фондовий ринок" від 23 лютого 2006 року № 3480-15, остання редакція від 27.07.2010: режим електронного доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3480-15

2. Рішення ДКЦПФР "Щодо затвердження Концепції запобігання маніпулюванню ринком цінних паперів, нечесній торговій практиці і порушенню етики професійної діяльності на фондовому ринку" від 14.01.2003 р. N21: режим електронного доступу: http://www.uaib.com.ua/files/articles/163/81_4.doc.

3. Ткачук Т. Шляхи запобігання та протидії промисловому шпигунству // Бизнес и безопасность. — 2007. — №3. — С. 7.

4. Скиба Б. Ю., Курбатов Б. А. Руководство по защите от внутренних угроз информационной безопасности — М.: издательство Питер, 2008. — 320 с.

5. Глушков В.О. Коваленко П.М. Шахрайство на фінансових ринках у біржовій торгівлі правовий та кримінологічний аналіз. — К.: Видавничий дім "Ін Юре", 2008. — 280 с.

6.Кавун С.В. Інформаційна безпека: навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Манжай. — Харків: Вид-во ХНЕУ, 2008. — 352 с.

Стаття надійшла до редакції 15.08.2010 р.