УДК 347.191.11:65.012.32 (045)

Ю. В. Біляк,
к. е. н., доцент кафедри менеджменту ім. Й. Завадського, НУБіП

ЕКОНОМІЧНА БЕЗПЕКА КОРПОРАЦІЇ — ЯК ЗАПОРУКА РОЗВИТКУ КОРПОРАТИВНОГО КОНФЛІКТУ

Y. Biliak,
PhD, Associate Professor Department of Management, NUBiP

ECONOMIC SECURITY OF CORPORATION — CORPORATE DEVELOPMENT AS A GUARANTEE OF CONFLICT

У статті розглянуто взаємозалежність економічної безпеки корпорації з корпоративними конфліктами, досліджуються підходи до формування цілей і завдань та їх роль у системі економічної безпеки підприємств; пропонуються системні і комплексні цілі та завдання, а також технологічні вимоги щодо їх визначення.

Обгрунтовано сутність економічної безпеки підприємства як складової системи корпоративного управління.

The article examines the interdependence of economic security corporation with corporate conflicts explored approaches to formulating goals and objectives and their role in the economic security companies; proposed system and comprehensive goals and objectives, as well as technical requirements for their determination.

The essence of economic security as a component of corporate governance.

Ключові слова: корпоративне управління, внутрішній конфлікт, перерозподіл власності, корпоративний конфлікт, економічна безпека підприємств.

Key words: corporate governance, internal conflict, redistribution of property, corporate conflict of economic security.

ПОСТАНОВКА ПРОБЛЕМИ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Проблема економічної безпеки отримує суттєвий розвиток в Україні з середини 90-хх років, коли молода держава і вітчизняні підприємства стикаються з необхідністю урахування ризиків в перехідній економіці; потребою своєчасної адекватної реакції на зміни з метою забезпечення адаптації всіх елементів системи до новітніх умов функціонування.

Основні повноваження і завдання всіх суб'єктів забезпечення системи національної безпеки, що визначені Конституцією України і Законом України "Про основи національної безпеки України", лише побічно торкаються проблеми організації безпеки суб'єктів підприємницької діяльності. Фактично господарюючі суб'єкти залишаються сам на сам зі своїм законним бажанням захисту власних інтересів, які, в кінцевому підсумку, становлять важливу складову загальнонаціональних інтересів, а від організації ефективної безпеки їхньої діяльності безпосередньо залежать міцність та перспективи розвитку України.

Уявлення про корпоративну безпеку за останні роки зазнало ряд змін. На початку дев'яностих акцент робився на захисті (охороні) підприємцями своєї власності і життя. Це визначалося високою криміналізацією бізнесу. Провідним фактором загрози був кримінал. Від нього можна було захиститися, використовуючи інженерно-технічні засоби і фізичну охорону. У цей момент з'являється велика кількість приватних охоронних підприємств і виникає інститут охоронців. Це дало очікуваний результат. Кількість нападів на об'єкти і розкрадань матеріальних цінностей істотно скоротилося.

Поступово, у міру розвитку ринкових відносин і посилення заходів правового регулювання ринку, акцент став переноситися у сферу економіки. Важкий податковий прес не давав бізнесменам можливості швидко розвиватися в рамках правового поля. У цей період не було практично жодного підприємства, яке працювало б без порушень чинного податкового законодавства. Внаслідок цього з'являється маса схем законної і незаконної мінімізації податків. Природно , що при такому положенні справ серйозним "фактором загрози" для бізнесу стали контролюючі та правоохоронні органи.

Формально використання таких схем можна віднести до системи заходів забезпечення економічної безпеки. Як і операції з повернення боргів. Ці заходи проводилися переважно силовими методами. Часто в їх реалізації ак-

Передплатний індекс 21847

тивну участь брали і співробітники правоохоронних органів. Для вирішення даного кола завдань на підприємствах і фірмах створювалися служби безпеки, на які було покладено обов'язки щодо забезпечення, насамперед, економічної та інформаційної безпеки.

У цей же час відбулися серйозні кадрові зміни в силових структурах. Частина співробітників звільнилася, частина перейшла в податкову службу та інші новоутворені структури. Пропозиція породила попит. Більшість звільнених знайшли застосування своєму досвіду та знанням в приватних охоронних підприємствах і комерційних структурах в якості керівників служб безпеки. Слід зазначити, що основним критерієм відбору служила кількість зв'язків в силових структурах, що залишилися у кандидатах на посаду. Таким методом "старих зв'язків" вдавалося знаходити потрібні контакти в правоохоронних та контролюючих органах.

Другим ефективним методом уникнути санкцій стали відкупи.

Прихід в комерційні структури колишніх співробітників силових структур призвів до того, що служби безпеки стали за своєю структурою нагадувати міні-копії МВС. Дана обставина не могла не відбитися і на методах роботи.

Основна увага при забезпеченні безпеки стала приділятися побудові системи охорони, захисту інформації та економіки. Багато бізнесменів вважають, що, створивши у собі службу безпеки і поставивши на чолі її колишнього співробітника МВС, вони можуть спати спокійно. Якоюсь мірою вони праві. При тому рівні розвитку ринку захист від оборони був найбільш ефективним.

Не так давно у Великобританії вибухнув скандал — жорсткі диски з даними пацієнтів клінік, які повинні були бути знищені, виявилися раптом на аукціонах eBay.

Лікарні передавали списані диски компанії — підряднику, яка, в свою чергу, користувалася послугами приватної особи.

Заповзятливий англієць, замість того щоб сумлінно виконати свої обов'язки — знищити носії — виставляв диски з даними на продаж.

У цьому випадку "слабкими ланками" можна назвати два пункти — внутрішня робота з співробітниками і технічний захист. До витоку привів занадто довгий ланцюжок посередників, внаслідок чого замовник навіть не був в курсі, хто безпосередньо займається знищенням дисків і чиї дії необхідно було проконтролювати. Крім того, вже сам факт, що лікарні передавали диски з незахищеними особистими даними пацієнтів третім особам — технічне упущення співробітників.

Відповідальний підхід до забезпечення корпоративної інформаційної безпеки допоміг би уникнути даної ситуації.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ И ПУБЛІКАЦІЙ

Дослідженню категорії "економічна безпека" присвячені праці Є. Олейнікова, М. Бендікова, А. Сухорукова, В. Ковальова, О. Ляшенко, О. Олексюка та ін. [1].

Аналізу проблем фінансової безпеки як складової системи корпоративного управління підприємством приділяється увага вітчизняними та іноземними дослідниками, серед яких варто відмітити: М. Єрмошенка, В. Катикало, О.М. Костюка, Р.К. Мітчела, Н. Пойда-Носик, П.Ю. Старюк, А.Дж. Сейнер, Е. Шуена, Й. Шумпетера тощо [2].

Питання продуктивності активів та ресурсів підприємства висвітлені в працях відомих як вітчизняних, так і закордонних вчених І. Бланк, Б. Лев, Гері Кокінз, О.Г. Мендрул, О.Б. Бутнік-Сіверський та ін.

Проте існує багато нерозв'язаних питань стосовно вибору показників і методів її оцінювання.

ПОСТАНОВКА ЗАВДАННЯ

Корпоративний сектор економіки в Україні функціонує і розвивається в умовах значної кількості дестабілізуючих чинників. Вони порізному впливають на окремо взяту корпорацію, внаслідок чого можуть спричинити втрати. Особливо на зменшення прибутку підприємства (з імовірністю від 10 до 40%) впливають недобросовісна конкуренція і протиправні дії кримінальних структур. Бізнесу в сучасних умовах прожити в ідеальному спокої, коли все ладиться і спирається, практично не можливо. Закони ринку і конкуренція цього не дозволять. Значить треба бути готовим до будь-яких несподіванок [3].

По суті, сучасна корпоративна безпека мало чим відрізняється від давньої. Змінюються лише реалії, в яких бізнесмени мають вести свою справу.

Аналіз практики соціально-економічних перетворень у нашому суспільстві вже сьогодні дозволяє визначити найвідчутніші ризики та загрози, з якими стикаються вітчизняні корпорації, як державні так і приватні, на сучасному етапі розвитку України.

Зокрема з їх переліку можна виділити наступні:

— підвищення рівня конкурентної боротьби за ринки збуту з боку вітчизняних та іноземних товаровиробників;

Передплатний індекс 21847

— значний рівень монополізації ринку, криміналізація окремих секторів економіки;

— недосконаліть законодавства, що регулює відносини у сфері підприємництва;

— недостатній рівень взаємної координації діяльності правоохоронних органів;

— відсутністю напрацьованих технологій та засобів організації національної економічної безпеки;

— існуюча практика недотримання конфіденційності комерційної інформації, незаконне одержання такої інформації, в т.ч. із застосуванням технічних засобів.

В аспекті розвитку питань, пов'язаних з системою управління підприємством, економічна безпека не часто знаходиться в центрі уваги.

Вважається, що ці дві категорії є несумісними як в розрізі кінцевої мети, так і методології.

Однак саме сутність завдань, що вирішує корпоративне управління на сучасному етапі розвитку економічних систем та зростання ризиків в діяльності підприємств, що є наслідком світових фінансово-економічних криз, визначає необхідність виявлення взаємозв'язків між зазначеними поняттями.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Будь-яка компанія хоче бути надійно захищена не тільки від зовнішніх загроз, а й від внутрішніх. Цю проблему і вирішують фахівці з корпоративної та інформаційної безпеки. Перед ними стоїть завдання проводити цілий комплекс заходів, що включають в себе практично всі сфери життя компанії:

1. Захист комерційної таємниці.
2. Внутрішня робота з співробітниками.
3. Внутрішня контррозвідка.
4. Службові розслідування.
5. Економічна безпека.
6. Технічний та фізичний захист.

У міру розвитку ринку та вдосконалення законодавства змінюються і методи управління бізнес — структурами. Відповідно, повинні змінюватися і підходи до забезпечення безпеки. З'явилася об'єктивна потреба в розробці нової концепції корпоративної безпеки. Основою нової концепції має стати саме системний підхід. Але перш ніж говорити про саму концепцію, було б доцільно розглянути деякі базові поняття. До них в першу чергу відноситься сам термін "безпека".

Підприємства індустріально і ринково розвинутих країн витрачають на управління економічною безпекою до 15% прибутку. Проте однією з основних перешкод на шляху формування ефективної системи корпоративної безпеки є багатоманітність підходів до розуміння сутності і змісту самого поняття "корпоративна безпека". Це, у свою чергу, негативно відображається на ефективності її забезпечення.

Сьогодні найбільш типовою є система безпеки, що складається зі служб охорони, економічної, інформаційної, інженерно- технічної безпеки. Кожне з перелічених напрямів має свою ідеологію і своїх ідеологів. Це призводить до того, що прихильники кожного з них намагаються довести, що саме їх напрям є найбільш важливим у забезпеченні корпоративної безпеки, формально визнаючи при цьому необхідність комплексного підходу.

Модель корпоративної безпеки будь-якої фірми схематично виражається просто. Елементи факторів ризику проявляються завжди в двох сферах, і виявити їх можна, як правило, за межами компанії і в ній самій. Спробуємо спрогнозувати ці можливі загрози.

Будь-яку фірму або організацію можна розглядати як окремий випадок відкритої системи. Дійсно, для того, щоб виробляти який-небудь продукт або послугу, організація повинна взаємодіяти з середовищем та іншими учасниками ринку. У зовнішньому середовищі існують дві групи факторів:

— позитивні, тобто сприяють розвитку бізнесу;

— негативні — ускладнюють його розвиток.

Останні прийнято називати факторами загрози, в яких міститься небезпека.

Специфіка чинників загрози полягає в тому, що, будучи об'єктивно зумовленими, вони не піддаються управлінню з боку служб безпеки. Таким чином, у бізнес-структур виникає необхідність у розробці ефективної системи заходів протидії факторам загрози в разі їх актуалізації.

Найбільш активними факторами загрози на цей час за оцінками великого числа опитаних бізнесменів у більш ніж 50 суб'єктах країни є:

а) конкуренти;

б) корумповані елементи держструктур;

в) кримінал;

г) техногенні катастрофи та природні катаклізми.

Більшість бізнесменів з усіх факторів загрози на перше місце ставлять конкурентів. Слід зазначити, що конкуренція — природний і навіть необхідний процес в умовах ринкових відносин.

У свою чергу, недобросовісна конкуренція породжує два нових фактора загрози:

— промислове шпигунство;

— рейд (недружні поглинання).

Передплатний індекс 21847

Самі по собі ці чинники пасивні і активізуються в момент отримання замовлення на їх послуги. На проведенні акцій промислового шпигунства, як правило, спеціалізуються приватні детективні агентства. На рейді — спеціально орієнтовані на цю діяльність фірми і компанії.

Істотний негативний вплив на розвиток, передусім, суб'єктів малого та середнього бізнесу надають корумповані співробітники численних перевіряючих і контролюючих органів, готові за певну винагороду закрити очі на виявлені в ході перевірок недоліки. У випадках недобросовісної конкуренції представники цього фактора загрози можуть стати пособниками однієї зі сторін, використовуючи адміністративний ресурс.

Що стосується криміналу, то бізнесмени різних рівнів вважають в даний час цей фактор загрози менш значущим і найбільш передбачуваним.

Статистика останніх років свідчить про недостатню увагу з боку бізнесменів до такого фактору загрози, як техногенні катастрофи.

Прийнято вважати, що питання забезпечення економічної безпеки є прерогативою служби безпеки, проте окрім неї в цьому процесі задіяний і ряд інших учасників, у тому числі:

1) топ-менеджмент;
2) служба внутрішнього аудиту;
3) інформаційно-аналітична служба;
4) служба персоналу;
5) юридична служба.

Аналогічна ситуація складається у відношенні інформаційної та соціальної безпеки. Така обставина диктує необхідність перегляду підходів як до побудови самої системи безпеки, так і до принципів управління нею.

Крім факторів зовнішньої загрози, на рівень корпоративної безпеки корпорації істотний деструктивний вплив надають і фактори внутрішньої загрози. Вони також володіють об'єктивною природою і фактично присутні на будь-якому підприємстві. При активізації ці фактори здатні підірвати компанію зсередини. Вони мають складну структуру і вимагають до себе не меншої уваги.

Фактори внутрішньої загрози відрізняє виражений суб'єктний характер. За кожним з них стоїть окрема людина або група осіб. При цьому один і той же працівник може одночасно розглядатися у складі двох і більше факторів загрози.

Наслідки для фірми в результаті актуалізації небезпек, які у різних факторах загрози, можуть істотно різнитися. На цій підставі можна умовно "вибудувати" якусь ієрархію внутрішніх факторів загрози. На першому, верхньому рівні знаходяться господарі або засновники фірми, так як само вони закладають "ген смерті" в тіло компанії. Тільки власник або засновник знають, для чого і на який термін створена фірма. Тільки вони можуть у будь-який момент відмовитися від свого бізнесу або від контрольного пакета акцій. Від них залежить стратегія формування концепції корпоративної безпеки фірми.

Другий рівень складають топ-менеджери. Від їх професіоналізму залежить як успіх, так і поразки фірми. Однією з передумов активізації рейду відносно підприємства є неефективне управління їм. Часто становище ускладнюється тим, що для російського бізнесу характерним є поєднання ролі власника з ролями генерального директора або президента компанії.

Третій рівень серед факторів внутрішньої загрози займає служба безпеки. Небезпеки, що містяться в цьому факторі загрози, виникають з двох першопричин. По-перше, це єдиний підрозділ компанії, функціональним завданням якого є підтримка на заданому рівні корпоративної безпеки. І, отже, від рівня професіоналізму її співробітників залежить досягнення чи недосягнення поставленої мети. По-друге, рівень безпеки безпосередньо пов'язаний з лояльністю співробітників служби по відношенню до фірми.

Четвертий рівень — служба персоналу. Як і у випадку зі службою безпеки, на рівень корпоративної безпеки у великій мірі впливатимуть професіоналізм її співробітників у сфері підбору персоналу, виявлення та вирішення конфліктних ситуацій. Саме в цій службі концентрується конфіденційна інформація про особистісні якості персоналу фірми.

Тобто матеріали, що представляють інтерес для конкурентів і криміналу.

П'ятий рівень внутрішніх загроз можна класифікувати як "групи корпоративного ризику". Ці групи, на відміну від раніше розглянутих, є умовними, тобто включаються до них співробітники об'єднані на підставі наявності у них загальної ознаки. При цьому вони можуть навіть не знати про свою приналежність до однієї з цих груп і особисто не контактувати один з одним.

До цих груп належать такі категорії працівників:

а) носії інформації, яка містить комерційну таємницю;

б) особи, що перебувають у стані конфлікту (рольового, особистісного, групового);

Передплатний індекс 21847

в) особи, які мають дорогі хобі, що захоплюються азартними іграми або екстремальними видами спорту;

г) нелояльні співробітники.

Небезпека, що міститься в цьому факторі загрози, має виражену особистісну природу і реалізується у формі навмисних або ненавмисних дій співробітників, здатних привести до зниження рівня корпоративної безпеки.

Так, наприклад, носії відомостей, що становлять комерційну таємницю, можуть стати джерелом інформації для конкурентів або за власною ініціативою, або в якості жертв маніпулятивних прийомів вивідування.

Що ж до співробітників, що перебувають у стані конфлікту будь-якого роду, то їх професійна надійність і лояльність в цей період різко падає. Досить часто, вирішуючи свої проблеми, вони здійснюють вчинки, що завдають серйозної шкоди корпоративній безпеці.

Особи, які мають дорогі хобі, що не відповідають їх фінансовим можливостям, можуть стати розтратниками казенних коштів або потрапити в боргову залежність. Це однаковою мірою відноситься і до любителів азартних ігор. Певну небезпеку являють собою і "екстрімали". Отримавши травму або каліцтво, вони можуть завдати фірмі великої шкоди через тривалий період непрацездатності.

Якщо розглядати лояльність як ступінь відданості групі, то всіх членів команди можна умовно розділити на три підгрупи.

Лояльні — ті, хто ні за яких умов не покине групу.

Ситуативно-лояльні — демонструють свою відданість груповим ідеалам тільки доти, поки досягнення загальних цілей не суперечить задоволенню їх особистісних інтересів.

Нелояльні — використовують своє перебування в команді тільки для задоволення своїх особистісних потреб, які реалізуються асоціальними і антисоціальними прийомами і методами. Слід зазначити, що, як правило, нелояльність має латентний (прихований) характер і виявляти її досить важко.

Отже, постає питання, що ж необхідно зробити, щоб отримати на виході реально працюючу систему інформаційного захисту.

Перш ніж приступати до побудови ефективної системи інформаційної безпеки, необхідно ретельно проаналізувати вже існуючу на підприємстві систему зберігання і обробки даних. Є три основні кроки, які необхідно для цього зробити:

1. Виявлення критично важливої інформації.

2. Виявлення слабких місць у корпоративній безпеці.

3. Оцінка можливостей захисту цієї інформації.

Усі ці дії можна виконати або силами своїх співробітників, або замовити у фахівців аудит інформаційної безпеки компанії. Переваги першого способу — нижча вартість і, що важливо, відсутність доступу до корпоративних даних для третіх осіб. Однак якщо в організації немає хороших штатних фахівців з аудиту безпеки, то краще всього вдатися до допомоги сторонніх компаній — результат буде надійніше. Це допоможе уникнути найбільш поширених помилок у забезпеченні інформаційної безпеки.

Найчастіші помилки — це недооцінка і переоцінка загроз підприємницької діяльності. У першому випадку, в системі безпеки підприємства зяють діри, що для організації обертається прямим збитком від витоку конфіденційної інформації, корпоративного шахрайства і відвертого злодійства що під руку попадеться.

При переоцінці загроз система безпеки не тільки важким тягарем лягає на бюджет підприємства, а й невиправдано ускладнює працівникам організації виконання покладених на них обов'язків. Це загрожує втратами можливого прибутку і втратою конкурентоспроможності.

Виявлення критично важливої інформації. На цьому етапі відбувається визначення тих документів і даних, безпека яких має величезне значення для компанії, а витік — зазнає величезних збитків. Найчастіше до такої інформації відносяться відомості, що становлять комерційну таємницю, але не тільки.

Наприклад, після прийняття нової редакції федерального закону "Про персональні дані" в охороні потребують і всі відомості, що збираються організацією про своїх співробітників і клієнтів.

Важливо пам'ятати: сторонні фахівці — аудитори не можуть самостійно скласти список всіх документів, які необхідно захищати. Робота аудитора повинна виконуватися спільно з співробітником підприємства, який добре знає особливості документообігу.

Виявлення слабких місць у корпоративної безпеки. Це завдання виконується безпосередньо фахівцями, які проводять аудит. Від результатів цієї роботи залежить вибір схеми побудови інформаційної безпеки.

При виявленні проломів в інформаційній та, як наслідок, корпоративній безпеці оцінюються не тільки технічні засоби. Дуже важливий момент — наявність розмежування прав доступу співробітників до тієї чи іншої інформації,

Передплатний індекс 21847

угоди про нерозголошення корпоративної інформації. Важливо також оцінити лояльність працівників до керівництва і взаємини в колективі — все це входить в обов'язки відділу по роботі з персоналом.

Недавній приклад ситуації, коли штатний співробітник скористався своїм становищем і викрав інформацію — крадіжка кенійським представництвом Google відомостей про стартапі Mocality (онлайн-база бізнес-інформації). Google був змушений принести офіційні вибачення постраждалим, а глава представництва, з вини якого стався інцидент, був зміщений зі своєї посади.

Оцінка можливостей захисту інформації. Це завершальний етап аудиту, в ході якого на підставі проведеного аналізу складається список конкретних заходів, які необхідно прийняти для охорони корпоративних секретів компанії. Рекомендації можуть носити як технічний, так і організаційний характер.

Інформаційна безпека — лише один з багатьох способів (нехай і найважливіший) забезпечити корпоративний захист. Необхідний комплекс заходів — технічних і організаційних.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ

У результаті проведеного дослідження щодо визначення сутності економічної безпеки як складової системи корпоративного управління підприємством доцільно зробити наступні узагальнення:

Отже, корпоративна безпека допомагає забезпеченню стану захищеності майнових інтересів власників бізнесу, систем гарантій і заходів, що забезпечують:

1) контроль власників за приналежністю ним компанії;

2) можливість своєчасного запобігання конфліктів із співвласниками, менеджментом;

3) наявності механізмів захисту в разі порушення прав власника бізнесу іншими особами.

Втім, однієї лише технічної безпеки даних і відстеження дій співробітників недостатньо. Важливі й організаційні заходи, робота з співробітниками, розробка внутрішньої документації.

Система корпоративної безпеки повинна бути комплексною.

Організаційна робота включає в себе інформування персоналу про наявність в організації систем інформаційної безпеки, про необхідність дотримуватися комерційну таємницю і можливі наслідки її розголошення як для компанії, так і для самого співробітника. Створення сприятливої робочої атмосфери — ще один ключовий момент організаційних заходів. Корпоративна безпека неможлива, якщо співробітники недовірливо поглядають один на одного. Така "холодна війна" буде неабияк гальмувати бізнес-процеси. Тому ще раз варто нагадати про важливу роль відділу по роботі з персоналом.

Що стосується розробки внутрішньої документації, то повинні бути чітко прописані обов'язки працівників, а також їх права доступу до тих або інших документів. Кожен відділ повинен виконувати покладені на нього завдання — не більше, але й не менше.

Не можна забувати і про такі, здавалося б, елементарні речі, як робота служби безпеки. Фізичний захист співробітників на робочих місцях — теж важлива частина корпоративної безпеки.

Тільки після організації такого двостороннього — технічного та організаційного — захисту, що не перебільшує і не зменшує загрози, можна створити надійний корпоративний захист компанії.

Література:

1. Аверічев І.М. Ресурсне забезпечення економічної безпеки підприємств водного транспорту [Електронний ресурс]. — Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=2530

2. Д'яконова І.І. Фінансова безпека як складова системи стратегічного управління підприємством [Електронний ресурс]. — Режим доступу: https:// www. irbis-nbuv.gov.ua/.../cgiirbis_64.exe

3. Федулова Л.І. Корпоративні структури в інноваційній діяльності: світовий досвід і можливості для України / Л.І. Федулова // Економіка і прогнозування. — 2004. — № 4. — С. 9—27.

References:

1. Averichev, I. M. (2013), "Resource providing economic security of companies of water transport", Efektyvna ekonomika, vol. 11, available at: http://www.economy.nayka.com.ua/?op=1&z=2530 (Accessed 14 Nov 2013).

2. D'iakonova, I.I. (2013), "Financial security as a component of strategic management", available at: https:// www.irbis-nbuv.gov.ua/.../cgiirbis_64.exe (Accessed 14 Nov 2013).

3. Fedulova, L.I. (2004), "Corporate structures in innovation: international experience and opportunities for Ukraine", Ekonomika i prohnozuvannia, vol. 4, pp. 9—27.

Стаття надійшла до редакції 13.02.2014 р.

Передплатний індекс 21847