1. Економіка та організація інноваційний діяльності: Підручник / О.І. Волков, М.П. Денисенко, А.П. Гречан та ін.; Під ред. проф. О.І. Волкова, проф. М.П. Денисенка. – К.: ВД "Професіонал", 2004. – 960 с. 2. Гуменюк О.Д. Участь держави у формуванні інноваційно-інвестиційного потенціалу // Фінанси України. – 2005. – № 5. – С. 51–59. 3. Чабан В.Г. Інноваційний потенціал підприємства та його оцінка // Фінанси України. – 2006. – № 5. – С. 142–148. 4. Потенциал инновационного развития предприятия: Монография / А.А. Епифанов и др. – Сумы, 2005. – 255 с. 5. Закон України "Про інноваційну діяльність". – 2002.

УДК 330.131.7:330.33.01

Н.Є. Селюченко, В.П. Кічор
Національний університет "Львівська політехніка",
кафедра економіки підприємства та інвестицій

ІНФОРМАЦІЙНИЙ РИЗИК В АНТИКРИЗОВОМУ УПРАВЛІННІ

В сучасних умовах питання антикризового управління є актуальними для будь-якого суб'єкта господарювання. Успішність антикризових заходів істотно залежить від ризиків, які можуть виникати в процесі їх реалізації. До таких ризиків належить інформаційний ризик. Визначено джерела формування інформаційного ризику на різних етапах антикризового управління та запропоновано перелік заходів щодо зниження його рівня.

Ключові слова: антикризове управління, інформаційний ризик, джерела ризику, система захисту інформації, способи зниження рівня ризику.

In the modern terms of question of anticrisis management are actual for the any subject of menage. Progress of anticrisis measures substantially depends on the risks which can arise up in the process of their realization. The informative risk belongs to such risks. In the article certainly sources of forming of informative risk on the different stages of anticrisismanagement and the list of measures is offered on the decline of his level.

Key words: anticrisis management, informative risk, risk sources, system of priv, methods of decline of risk level.

Постановка проблеми

Управлінські рішення доволі часто приймають в умовах інформаційної невизначеності, викривлення інформації чи витоку конфіденційної інформації. Ці чинники є джерелами інформаційного ризику, який може спричинити певні втрати для суб'єктів господарювання. Наслідки його можуть бути навіть катастрофічними, особливо для тих підприємств, в діяльності яких вже спостерігаються кризові явища. З метою недопущення чи пом'якшення негативних наслідків інформаційного ризику постає необхідність його врахування під час управління як успішно функціонуючим підприємством, так і тим, що перебуває в кризовій ситуації.

Аналіз останніх досліджень і публікацій

Дослідженням проблем врахування інформаційного ризику під час управління розглядаються у працях багатьох фахівців в галузі економіки, математики, інформаційних технологій. Зокрема, поглиблено поняття інформаційного ризику, визначено роль системи внутрішнього контролю й аудиту в зменшенні інформаційного ризику користувачів фінансової звітності в роботі Н.І. Дорош,

питання управління інформаційним ризиком в електронному бізнесі розглядають А.В. Бєгун та А.В. Коноцера, способи захисту інформації в інформаційних системах пропонують Г. Мельник, В.О. Бондаренко, О.В. Литвиненко та ін., формуванню якісної інформаційної бази для прийняття антикризових управлінських рішень присвячені праці О.О. Терещенка, В.П. Мартиненка.

Разом з тим інформаційний ризик в антикризовому управлінні сьогодні залишається мало вивченим, що в умовах збитковості значної кількості вітчизняних підприємств та орієнтації економіки на інформаційно-інноваційні моделі розвитку є актуальним.

Постановка цілей

Дослідження теоретичних основ та прикладних проблем врахування інформаційного ризику під час антикризового управління зумовлює постановку таких цілей:

визначити джерела інформаційного ризику;

запропонувати способи зниження інформаційного ризику.

Виклад основного матеріалу

Антикризове управління, на думку фахівців, передбачає два рівні [2, с.15]: перший – комплекс профілактичних заходів з метою недопущення кризових ситуацій; другий – система заходів щодо виведення підприємства з кризової ситуації.

На кожному з цих етапів джерела інформаційного ризику, його допустимий рівень та способи зниження є різними.

Для здійснення попереджувальних заходів щодо недопущення кризових явищ на підприємстві має функціонувати система раннього попередження та реагування. Вона є елементом антикризового фінансового контролінгу і завчасно виявляє можливі ризики, загрози для нормальної діяльності підприємства, прогнозує фінансовий стан, а також виявляє й оцінює додаткові фактори успіху. З цією метою використовують такі методи, як комплексний аналіз фінансових коефіцієнтів, кореляційний аналіз, дискримінантний аналіз, розроблення сценаріїв, СВОТ-аналіз.

Вже на етапі оцінювання фінансового стану підприємства та можливості його банкрутства виникає інформаційний ризик.

Джерелом інформаційного ризику насамперед може бути офіційна документація підприємства, оскільки вона може містити помилки, випадково чи навмисне викривлену інформацію, що особливо характерно для підприємств, які перебувають у кризових ситуаціях.

У [3] зазначено, що під час аналізу 40 фінансових звітів (форми 1 та 2) вітчизняних підприємств, які функціонують нормально, та 40 звітів підприємств-банкрутів встановлено, що в переважній більшості фінансових звітів (більше ніж у 2/3) підприємств з обох груп значення багатьох показників дорівнюють нулеві, зокрема, до таких показників належать чистий прибуток, грошові засоби та їх еквіваленти.

Крім того, зовнішня звітність підприємств, як правило, складається без дотримання або за умови часткового застосування загальновизнаних принципів бухгалтерського обліку. Національна система бухгалтерського обліку та звітності і звітність інших країн характеризуються такими розбіжностями [4]: невідповідність обсягу і змісту інформації у звітах; відмінності у структурі фінансових звітів; різні підходи до оцінки статей фінансової звітності. Це ускладнює використання моделей аналізу фінансового стану підприємств, розроблених зарубіжними вченими.

Такі моделі також не можуть бути використані для діагностики фінансового стану українських підприємств, оскільки умови їх господарювання істотно відрізняються. Так, зокрема, сьогодні відома значна кількість моделей багатофакторного дискримінантного аналізу, розроблена фахівцями різних країн. Однак, як зазначають вітчизняні науковці [3], коефіцієнти дискримінантних моделей різко змінюються рік у рік і від країни до країни.

Автором [3] проведено низку експериментів щодо визначення точності прогнозування банкрутства підприємств з застосуванням моделей багатофакторного дискримінантного аналізу, розроблених науковцями різних країн. Зокрема, модель Терещенка О.О. [2, с.104–122], розроблена для українських компаній, не була здатна ідентифікувати фінансовий стан 51,4 % аналізованих

підприємств, попри те, що усі показники було попередньо опрацьовано згідно з встановленими рекомендаціями. Серед компаній, стан яких було класифіковано як фінансово стійкий, помилок в ідентифікації зроблено не було. У той самий час серед ідентифікованих підприємств, яким загрожує банкрутство, точність класифікації становила всього 15,4 %. З урахуванням компаній з нерозпізнаним фінансовим станом точність класифікації підприємств-банкрутів знижується до 5,4 %. Отже, точність класифікації серед ідентифікованих компаній сягає 67,6 %, а для усієї множини аналізованих підприємств – знижується до 32,9 %. Внаслідок проведених досліджень А. Матвійчуком розроблено дискримінантну та нечіткі моделі аналізу фінансового стану та оцінки ймовірності банкрутства підприємства, які мають доволі високу точність передбачення банкрутства вітчизняних підприємств. Однак, як зазначає автор, «...проведене дослідження збереже силу доти, доки законодавча база української економіки не зазнає кардинальних змін. У такому разі доведеться здійснити новий відбір факторів впливу, переформувати набір логічних правил і провести переналаштовування параметрів моделі на новій навчальній вибірці».

Усе вищезазначене свідчить про те, що не можна механічно використовувати методи та моделі для аналізу фінансового стану підприємств в умовах, що характеризуються інформаційною невизначеністю та динамічно змінюються. Використання таких моделей також є джерелом інформаційного ризику.

На етапі попередження кризових явищ сьогодні актуальним є завдання своєчасного виявлення загроз недружнього захоплення підприємства – рейдерства. Одним з методів захисту від рейдерства є моніторинг інформаційного середовища навколо підприємства з метою виявлення до нього небажаного інтересу. Характерними індикаторами загрози захоплення підприємства можуть бути спроби скуповування частини акцій компанії, вимоги міноритаріїв про проведення позачергових зборів акціонерів, заперечення акціонерів проти угод компанії, несподівані перевірки підприємства контрольно-наглядовими органами, факти злиттів і поглинань підприємств у цьому регіоні або у цій галузі. Штучне банкрутство та початок процедури санації також є однією зі схем захоплення підприємств [5]. Отже, джерелом інформаційного ризику в цьому випадку може бути несвоєчасна та неточна інформація щодо зазначених індикаторів, внаслідок чого підприємство може бути захоплене рейдерами.

В умовах антикризового управління, метою якого є виведення підприємства з кризи, забезпечення ефективності його діяльності та конкурентоспроможності в довготерміновому періоді, інформаційну базу прийняття управлінських рішень необхідно доповнити блоком даних, які використовують для розроблення та реалізації плану санації.

План санації має містити: аналіз фактичного фінансового стану підприємства; аналіз причин кризової ситуації та слабких місць; оцінку стану ринків збуту продукції; аналіз галузі, конкурентоспроможності підприємства та його продукції; оцінку наявного потенціалу; план маркетингу; план виробництва та капіталовкладень; організаційний та фінансовий плани; оцінку ризиків реалізації плану та його ефективності.

Розроблення будь-якого з перерахованих блоків плану санації пов’язане з інформаційним ризиком. Інформаційний ризик може бути зумовлений відображенням неповної інформації про фінансовий стан та внутрішньогосподарські процеси, недоступністю інформації щодо кон’юнктури товарного та фінансового ринків, відсутністю інформації про бізнес-середовище, асиметрією інформації, непрогнозованими змінами законодавства тощо. Внаслідок цього можуть бути допущені помилки у виборі антикризової стратегії, джерел фінансування санаційних заходів, розробленні виробничо-технічних, організаційно-правових, соціальних заходів тощо, що унеможливить виведення підприємства з кризової ситуації.

Інформаційний ризик може слугувати джерелом інноваційних ризиків, пов’язаних з інноваційними процесами на підприємстві.

«Досягти необхідного рівня конкурентоспроможності можуть лише ті підприємства, які вчасно реагують на інноваційні вимоги нової економіки, успішно розв’язують завдання фінансового забезпечення та якісної інформаційної підтримки відповідних управлінських рішень. Усі інші господарські структури опиняються у стані перманентної боротьби за виживання» [6].

В антикризовому управлінні можна використовувати такі види інновацій: процесні, продуктові, аллокаційні [7].

Процесні інновації – це нововведення у процеси взаємодії підприємства з зовнішнім середовищем, процеси управління рухом матеріальних запасів і грошових коштів на підприємстві, процеси загального менеджменту, технологічні процеси випуску продукції. Інформаційний ризик реалізації інновацій такого виду може бути зумовлений насамперед недостатнім рівнем компетентності антикризового менеджменту, неврахуванням різних внутрішніх та зовнішніх чинників.

Продуктові інновації полягають у виборі й освоєнні нових видів діяльності, продуктів. Для їх реалізації підприємству потрібне попереднє розроблення нового продукту та технології його випуску. Такі інновації можуть бути реалізовані власними силами підприємства чи шляхом замовлення у розроблювача. Перший варіант пов'язаний з інформаційним ризиком, джерелом якого може бути неправильна оцінка інноваційного потенціалу підприємства. Другий варіант – з інформаційним ризиком, зумовленим асиметрією інформації: інноваційна організація – продавець нововведення знає про нього більше, ніж замовник, який не має змоги перевірити його раніше, ніж здійснить угоду.

Аллокаційні інновації полягають в різних схемах реорганізації підприємства, перерозподілі (реструктуризації) матеріальних, фінансових і нематеріальних активів підприємства, перерозподілі відповідальності працівників підприємства, і, особливо, його менеджерів. Інновації такого виду є найдорожчими і найскладнішими в реалізації, повільно окуповуються. Від них можна очікувати як високого і тривалого ефекту, так і радикального всеохоплюючого провалу. Тому рівень інформаційного ризику у разі реалізації аллокаційних інновацій є найвищим порівняно з іншими видами інновацій. Джерелом інформаційного ризику в цьому разі є неповні та неточні дані про фінансово-майновий стан підприємства, якісні характеристики його працівників.

На сучасному етапі, коли спостерігається бурхливий розвиток інформаційних технологій, інформаційний ризик пропонують також аналізувати у зв’язку зі створенням інформаційних систем. В цьому контексті під інформаційним ризиком розуміють вірогідну частоту і вірогідну величину майбутньої втрати, що виникає внаслідок комбінації загрози, вразливості і особливості інформаційного активу [8].

Для оцінки загроз рекомендують використовувати такі чинники: статистику по зареєстрованих інцидентах; тенденції в статистиці за подібними порушеннями; наявність в системі інформації, що являє собою інтерес для потенційних внутрішніх або зовнішніх порушників; моральні якості персоналу; можливість отримати вигоду зі зміни оброблюваної в системі інформації; наявність альтернативних способів доступу до інформації; статистику щодо подібних порушень в інших інформаційних системах організації.

Вразливість можна оцінювати з урахуванням таких чинників: кількість робочих місць (користувачів) в системі; кількість осіб в робочих групах; обізнаність керівництва про дії співробітників (різні аспекти); характер устаткування і програмного забезпечення, яке використовують на робочих місцях; повноваження користувачів.

Ще одним чинником інформаційного ризику сьогодні є розвиток електронного бізнесу. Основні нові джерела ризиків е-бізнесу формулюють так [9]:

– зростаюча потреба безпечного і дозволеного доступу більшої кількості людей до інформаційної системи підприємства; багато з цих людей є “чужинцями” для цієї організації: у неї відсутній досвід спілкування з ними і вони можуть діяти через небезпечні комунікаційні мережі;

– Інтернет надає багато нових можливостей для е-бізнесу, потребує виконання високих стандартів; ці стандарти постійно розвиваються, але вони ще не досконалі і створюють нові джерела для ризиків;

– поява інфраструктури безпеки комунікаційних систем кодування (паролі, коди, смарт-карти, тощо) ще недостатньо надійна і не створює умови для безпечного е-бізнесу;

– Інтернет-бізнес збільшує взаємозалежність між партнерами; це, з одного боку, добре, а з іншого, – небезпечно: можливі великі мережеві реакції, які знижують інтереси партнерів, споживачів, конкурентів, інвесторів, суспільства тощо;

– Інтернет не рахується з кордонами і суверенітетами, що може загрожувати сплаті податків, встановленню юрисдикції, залученню до відповідальності тощо.

Отже, з розвитком інформаційних технологій та е-бізнесу зростає ймовірність викривлення інформації, витоку конфіденційної інформації, що може бути використано конкурентами з метою послаблення ринкових позицій підприємства, його поглинання чи незаконного захоплення.

Визначення джерел інформаційного ризику вимагає розроблення рекомендацій щодо зниження його рівня.

У загальній системі захисту інформації виділяють такі напрями [10]:

– законодавчо-нормативне забезпечення передбачає розроблення відповідних законодавчих актів, нагляд за виконанням законодавства з боку правоохоронних органів, судовий захист;

– організаційно-технічне забезпечення розкриває систему заходів, спрямованих на недопущення реалізації загроз безпеці інформаційного ресурсу;

– страхування інформаційних ризиків, що прийнятне лише для недержавних установ (цей вид діяльності не дуже розповсюджений на теренах України, хоча експерти прогнозують йому великі перспективи розвитку, що зростатимуть відповідно до збільшення обсягів інформації, якою оперує суспільство).

Законодавча база у галузі безпеки інформації складається з законів України «Про інформацію», «Про захист інформації в автоматизованих інформаційних системах», «Про державну таємницю» тощо. Діє також низка Указів Президента та Постанов Кабінету Міністрів України, які регулюють конкретні напрями діяльності в галузі захисту інформації.

Враховуючи напрацювання вітчизняних та зарубіжних науковців в напрямку зниження інформаційного ризику, рекомендуємо підприємствам реалізувати такі заходи:

– ретельний підбір персоналу, зокрема управлінського, з урахуванням таких його характеристик, як професіоналізм, компетентність, креативність, конформізм, конструктивність мислення, колективізм, самокритичність, відповідальність;

– формування інформаційної бази прийняття управлінських рішень на основі таких принципів, як актуальність, достовірність, надійність, релевантність, цілеспрямованість та інформаційна єдність даних, повнота відображення змісту, зрозумілість;

– використання не одного, а декількох надійних інформаційних джерел для підвищення якості інформаційного забезпечення;

– формування блока антикризової інформації, який міститиме оперативні дані про «вузькі місця», потенційні небезпеки та загрози (індикатори кризового стану); з цією метою періодично необхідно проводити внутрішній контроль та аудит, а також постійний моніторинг зовнішнього середовища;

– використання додаткової інформації у разі недостатності наявної для прийняття обґрунтованих рішень;

– нагромадження, аналіз та ефективне використання інформації про досвід діяльності зарубіжних підприємств, науково-технічні досягнення;

– впровадження організаційно-технічних заходів, спрямованих на недопущення несанкціонованого доступу до інформації та її модифікації, витоку інформації, знищення чи порушення її цілісності.

Зазначимо, що частина з цих заходів вимагає значних фінансових ресурсів, що є вкрай важливим для підприємства, яке перебуває в кризі. Тому прийняття рішення щодо вибору способів зниження інформаційного ризику повинно враховувати: вартість здобуття додаткової інформації; важливість інформації, яку захищають; величину збитків, які може спричинити втрата інформації; ефективність інформаційної системи і системи захисту та їх відповідність вартості.

Висновки

1. З метою вдосконалення підходів до зниження рівня ризиків в процесі антикризового управління нами вибрано інформаційний ризик, який має значний вплив на прийняття рішень на різних етапах антикризового управління. Під час дослідження виділено такі джерела

інформаційного ризику: офіційну документацію підприємства; методи та моделі для аналізу фінансового стану підприємств; асиметрію інформації; недосконалу інформаційну інфраструктуру, наслідком чого може бути: несвоєчасна та неточна інформація про фінансовий стан та внутрішньо-господарські процеси, кадровий потенціал, бізнес-середовище підприємства, недоступність інформації щодо кон'юнктури товарного та фінансового ринків; непрогнозовані зміни законодавства; створення інформаційних систем; розвиток електронного бізнесу.

2. Для зниження рівня інформаційного ризику запропоновано здійснювати ретельний підбір персоналу, вдосконалювати формування інформаційної бази прийняття управлінських рішень, використовувати декілька надійних інформаційних джерел, формувати блок антикризової інформації, використовувати додаткову інформацію, вивчати зарубіжний досвід та науково-технічні досягнення, забезпечувати захист інформації в інформаційних системах та в електронному бізнесі.

Перспективи подальших досліджень

Виділені джерела інформаційного ризику та способи зниження його рівня будуть використані в подальших дослідженнях стосовно визначення допустимого рівня ризику на різних етапах антикризового управління, а також доступних заходів його зниження з урахуванням фінансового стану підприємства та витрат, необхідних для їх реалізації.

1. Дорош Н.І. Методологічні та організаційні аспекти аудиту: Автореф. дис…. д-ра екон. наук: 08.06.04 / Національний науковий центр «Інститут аграрної економіки». – К., 2004. 2. Терещенко О.О. Антикризове фінансове управління на підприємстві: Монографія. — К.: КНЕУ, 2004. – 268 с. 3. Матвійчук А. Дігностика банкрутства підприємств // Економіка України. – 2007. – №4. – С.20–28. 4. Буряк П.Ю. Формування і надання інформації про фінансові ресурси підприємства // Фінанси України. – 2006. – №10. – С.123–128. 5. Паламарчук Г., Венгер Л. Особливості рейдерства в Україні та політика його подолання // Економіка України. – 2007. – №9. – С.38–45. 6. Терещенко О.О. Антикризовий фінансовий менеджмент – вимога «нової економіки // www. corporation. org. ua / library/publication. 7. Валдайцев С.В. Антикризисное управление на основе инноваций: Учеб. пособие. – СПб.: Изд-во С.-Петербург. ун-та, 2001. – 232 с. 8. Мельник Г. Моделювання процесу управління інформаційними ризиками із застосуванням технології оцінювання можливих загроз та вразливості інформаційної системи // www.rusnauka.com/13.DNI_2007/Economics. 9. Бєгун А.В., Коноцера А.В. Інформаційний ризик в е-бізнесі // nc.ufei.ukrsat.com/Kyrsi%202004/tezi/images_tezi. 10. Бондаренко В.О., Литвиненко О.В. Інформаційна безпека сучасної держави: концептуальні роздуми // www.niurr.gov.ua/ukr/publishing/panorama1. 11. Мартиненко В.П. Стратегія життєздатності підприємств промисловості: Навч. посібник. – К.: Центр навчальної літератури, 2006. – 328 с.