https://economics.unian.ua/agro/2338678-agrosektor-formue-17-18-ukrajinskoji-ekonomiki-groysman.html (access date January 10, 2018).

2. Khalina, V. (2014), "The methodical approach to the assessment of the level of economic security", available at: http://chtei-knteu.cv.ua/herald/content/download/archive/2014/v1/NV-2014-V1_22.pdf (access date January 12, 2018).

3. Balaniuk, I. and Maksymiuk, M. (2016), "Essence of economic security of the enterprise", *Innovative economy*, no. 1-2, pp. 246-251.

4. *Bezpeka* [Security], available at: https://uk.wikipedia.org/wiki/Безпека (access date January 12, 2018).

5. Mishchenko, S.G. (2004), "The system of economic security of the organization", diss. ... candidate econ sciences, Rostov-on-Don, Russia, 197 p.

6. Kozachenko, H., Ponomarov, V. and Liashenko, O. (2003*), Ekonomichna bezpeka pidpryiemstva: sutnist ta mekhanizm zabezpechennia* [Economic security of enterprise: the gist and mechanism to providing], monograph, Libra, Kyiv, Ukraine, 280 p.

7. Evdokimov, F., Mizina, O. and Borodin, A. (2002), "Generalizing assessment of the financial component of economic security", *Scientific Papers of Donetsk National Technical University*, Donetsk: DonNTU, Vol. 47, pp. 6-12.

8. Hryshko, N. (2013), "Formation of the estimated parameters of the economic safety components of the machine-building enterprise*", Bulletin of socio-economic research*, no. 1, pp. 62-69.

9.Mishchenko, S.P. (2011), "Conceptual aspects of economic security companies in a market economy", *Marketing and Innovation Management*, no. 2, pp. 190-195.

10.Aziz, M. and Dar, H. (2006), Predicting Corporate Bankruptcy - Where Do We Stand?, *Corporate Governance Journal,* Vol. 6, No. 1, pp. 18-33.

11.Kovalenko, A. (2015), "Methodical provision of prediction of the probability of bankruptcy of agricultural enterprises", *Bulletin of the Khmelnitsky National University*, no. 3, Vol. 3, pp. 94-99.

Стаття надійшла до редакції 20.01.2018 р.

УДК 330.131.7

Кораблінова І.А.,
канд. екон. наук, доцент, докторант кафедри управління проектами та системного аналізу,
Одеська національна академія зв'язку ім. О.С. Попова

«ЦИФРОВА ТРАНСФОРМАЦІЯ» ЯК ДЖЕРЕЛО РИЗИКУ КОМПАНІЙ У СУЧАСНИХ УМОВАХ

Korablinova I.A.,
cand.sc.(econ.), assoc. prof., doctoral student at the department of project management and systems analysis,
Odessa National Academy of Telecommunications named after A.S. Popov

«DIGITAL TRANSFORMATION» AS A SOURCE OF RISK COMPANIES IN MODERN CONDITIONS

Постановка проблеми. Ідея «цифрової трансформації» охопила сьогодні думки мільйонів людей з наукового та ділового середовища. За останні декілька років у світ вийшли тисячі наукових публікацій, оглядів та звітів від практикуючих експертів, які присвячені різним аспектам «цифрової трансформації» компаній, освітніх організацій та ін. В Україні інтерес до цієї теми був активізований у 2016–2017 роках у межах знайомства з європейськими програмами та стратегіями розвитку (зокрема, «Digital agenda for Europe», «Industrie 4.0» (Німеччина) та ін.).

Слід відзначити, що сьогодні увага здебільшого приділена широким можливостям від впровадження нових цифрових технологій та вирішенню питань, які виникають під час інтеграції компаній у «цифрову екосистему». Проте, як показує практика, у процесі такої інтеграції перед її учасниками виникає низка нових проблем, які потребують осмислення та вирішення. Однією з них є значне посилення впливу невизначеності, пов'язаної з використанням нових технологій, та породжуваного нею ризику на кінцеві результати діяльності вітчизняних компаній, а також на розвиток економіки країни в цілому.

Аналіз останніх досліджень і публікацій. Сьогодні майже всі професійні спільноти, інтереси яких пов'язані з сферою новітніх інформаційних та комунікаційних технологій, представники IT-компаній, консалтингових агенцій розпочали активну відкриту дискусію та пошук шляхів приближення до нового технологічного рівня, про який оголошено на численних міжнародних заходах. Тільки у 2016–2017 роках такими міжнародними організаціями та корпораціями як World Economic Forum, Forrester, Microsoft, AAJ Technologies, FA Service, IBM, IDC були організовані десятки заходів з питань цифрової трансформації у різних країнах світу, зокрема в Україні.

Основна ідея, яка пронизує більшість публікацій та доповідей у зазначеній сфері полягає у тому, що на сучасному етапі розвитку глобальної економіки цифровізація є необхідною умовою для економічного зростання та підвищення конкурентоспроможності як окремих організацій, так і всіх країн світу.

Можна спостерігати, як у діловому середовищі інформаційні потоки наповнюються великою кількістю публікацій про необхідність здійснити «цифрову трансформацію» кожній компанії, яка бажає бачити себе у «цифровому майбутньому» [1–5]. Бібліотеки компаній, орієнтованих на інновації, поповнюються низкою таких бестселерів. Їх вивчають та обговорюють співробітники компаній, учасники практичних конференцій, ділових форумів, а також студенти освітніх програм з бізнесу, економіки та менеджменту.

Зокрема, на сайтах Microsoft, Amazon та ін. серед нової бізнес-літератури з'явилась низка книг з тематики «цифрової трансформації», які закликають читачів змінити свій тип мислення й приготуватись до змін у цифровій епосі. Як приклад можна навести роботу Д. Роджерса (2016) [1], в якій надано інструкцію для традиційних компаній на шляху «цифрової трансформації». Передусім, як радить автор, цим компаніям слід модернізувати стратегічне мислення та змінити відношення до клієнтів, конкуренції, даних, інновацій, цінностей тощо.

Червоною стрічкою через зазначену роботу проходить заклик бізнес-консультанта змінювати підходи до формування команд, експериментувати для виявлення кращих ідей та рішень, бути відкритими, інтегруватись у мережі та використовувати їх як ресурс. Слід зазначити, що ці ідеї вже не одне десятиліття пронизують тексти популярної ділової літературі, а сьогодні вони висвітлюються з позицій необхідності цифрових перетворень у діяльності компаній. Наприклад, їх можна побачити й у роботі «Цифрова матриця» (2017) [2]. Тут автор також наголошує, що у світі вже багато компаній стали цифровими, але це треба зробити й іншим компаніям, щоб не відставати від змін своєї галузі. Для цього компаніям пропонується пройти низку етапів, які навчать орієнтуватись у світі «цифрових екосистем» і знайти своє місце на новому «цифровому ландшафті».

Отже, сьогодні увага, здебільшого, приділена вражаючим можливостям впровадження цифрових технологій та переходу на цифрові платформи. Проте, як показує практика, компанії, які розпочали цей шлях, зустрічаються із низкою проблем. Звертаючи увагу на це, дослідник з Німеччини [6] на конференції IEEE з комп'ютерних наук та інформаційних систем зазначає, що управління безпекою та забезпечення безперервності діяльності компаній стає не тільки сферою IT-фахівців, ці питання тепер пронизують всю компанію, адже атаки та загрози ззовні та зсередини будуть «нормальним» явищем.

У світлі розглянутої проблеми цифрових перетворень, які здійснюються у компаніях останнім часом, виникає необхідність й далі продовжувати дослідження інформаційно-мережевої природи та форм взаємодії учасників нових цифрових екосистем у різних аспектах їх діяльності. Слід зазначити, що у даному контексті у літературі, як правило, розглядаються інформаційні ризики, які пов'язані із можливістю втрати цінних для компанії даних. Найбільше розробок з цього питання зустрічається серед представників технічних спеціальностей, зокрема фахівців з інформаційної безпеки, які пропонують конкретні технології діагностики та захисту інформації у рамках превентивного управління мережами. Разом з тим, по мірі реалізації концепції «цифрової трансформації» посилюється соціалізація компаній, що викликає необхідність дослідження нових загроз й з боку соціальних та поведінкових наук. Проте, у науковій літературі це питання ще недостатньо розвинуто.

Постановка завдання. Метою даної статті є визначення та обґрунтування існуючих проблем якісного аналізу ризиків компаній, які обрали шлях «цифрової трансформації» та знаходяться в умовах постійного оновлення інформації.

Виклад основного матеріалу дослідження. Якщо детально розглянути публікації та доповіді, що обговорюються останні декілька років на численних форумах та конференціях в сфері розвитку та застосування інформаційних та комунікаційних технологій, можна замітити, що в основі концепції «цифрової трансформації» лежить ідея переходу до нових цифрових платформ, через які будуть

відбуватись відносини між людьми, організаціями, державою тощо. При цьому йдеться не тільки про організаційно-технічний перехід на цифрові платформи (який передбачає нові можливості для інноваційного розвитку), але й про масштабні трансформації у соціальних та економічних відносинах.

Сучасні дослідники, зокрема Редді С. та В. Рейнарц [7], констатують, що цифрові перетворення торкаються тепер не тільки сфери інформаційних та комунікаційних технологій, і не тільки мають очевидний вплив на економічні системи та поведінку її учасників, але все частіше здійснюють революційний вплив на людей та суспільство у цілому: цифрові технології зменшують витрати на взаємодію, а чим більше обмінів, тим вище потенційні вигоди. У свою чергу, перехід до мережевих форм обміну передбачає, що кількість з'єднань в економічних та соціальних системах буде зростати експоненційно. Незважаючи на те, що автори окрім можливостей, які несе «цифрова трансформація», звертають увагу й на певні загрози, які пов'язані з новими змінами, для споживачів, компаній, кожної окремої людини та суспільства у цілому, вони все одно позитивно оцінюють ці перетворення і закликають їх прискорювати.

Втім, на нашу думку, вітчизняні компанії, які ще не мають достатньої захищеності від загроз зовнішнього середовища, можуть, скориставшись наполегливою рекомендацією здійснити «цифрову трансформацію», зробити такі кроки, які нанесуть збитки не тільки їм, а й вітчизняній економіці взагалі. Отже, маючи на меті долучитись до світового тренду всебічної цифровізації, слід розуміти, чи є сьогодні у компанії готовність приймати нові удари.

Якщо розглядати природу нових загроз, які очікують ту чи іншу компанію на шляху «цифрової трансформації», то передусім слід враховувати, що всі її дії будуть залежати від інформації, яка буде надходити з нових цифрових систем, до яких вона інтегрується.

У зв'язку з цим важливо розуміти, що діяльність компанії пов'язана із різними типами інформації, серед яких можна виділити такі: внутрішня та зовнішня; достовірна та недостовірна; повна та неповна; нова та застаріла; первинна та вторинна; структурована та неструктурована; потрібна та зайва; поточна (оперативна), стратегічна, минула та майбутня (прогнозна); комерційна та некомерційна; суттєво важлива, важлива, частково важлива, неважлива; відкрита, закрита, таємна; власна, споживча, партнерська, конкурентна, громадська; короткострокова, середньострокова, довгострокова; галузева, регіональна, кластерна, національна (країни базування), міжнародна; стандартизована, аналітична, статистична; перевірена та неперевірена; корпоративна, управлінська, індивідуальна; професійна, непрофесійна; проста, складна, адаптована, суперечлива і т.ін.

Здібність розуміти, якою інформацією оперує компанія у своїй діяльності при вирішенні тих чи інших питань, на наш погляд, є однією з ключових компетенцій компанії в умовах її інтеграції у ту чи іншу глобальну інформаційну систему, під час включення у ту чи іншу локальну цифрову екосистему, при переході на власні цифрові платформи і т.ін.

Оскільки цифрові перетворення пов'язують із розробкою та впровадженням інформаційно-комунікаційних технологій, під якими розуміють сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збору, обробки, збереження, поширення, відображення та використання інформації в інтересах її користувачів, ризики, що виникають у процесі цих перетворень, отримали назву «інформаційні».

Як було показано у роботі [8], інформаційні ризики проявляються (виникають) на різних ієрархічних рівнях – держави, економіки в цілому, корпораціях, окремих підприємствах тощо. Кожному рівню притаманний свій склад ризиків, що утворюють обсяг поняття «інформаційний ризик», який відбиває особливості його прояву на даному рівні, та враховує певні умови його функціонування. Так, наприклад, незважаючи на те, що проблема ризиків, пов'язаних з використанням інформації та інформаційних технологій є відносно новою у загальній теорії ризиків, деякі з них вже включено до переліку глобальних ризиків, які загрожують людству, та з якими воно поки що не в змозі впоратися [9].

Спираючись на праці [10; 11], слід відзначити, що перше питання, яке повинно бути вирішеним у процесі аналізу ризиків будь-якого об'єкту, є виявлення та ідентифікація усіх можливих ризиків, які можуть йому загрожувати (виникати) за певних умов його функціонування. Це завдання найбільш успішно дозволяє вирішити наявність класифікації ризиків об'єкту, що аналізується, яка повинна включати усю множину ризиків, що утворюють поняття його «обсягу». В подальшому, з цієї множини вибираються ті ризики, які відбивають особливості умов функціонування конкретного об'єкту. Так, наприклад, якщо компанія не отримує та не надає кредитів, їй не загрожує кредитний ризик, якщо не здійснює зовнішньоекономічну діяльність, їй не загрожує ризик країн і т.ін.

Зважаючи на сказане вище, для компаній, основна діяльність яких безпосередньо пов'язана із виробництвом (створенням), збереженням, передачею, розповсюдженням, зберіганням, обміном, споживанням інформації, кожна фаза відрізняється своїм набором інформаційних ризиків, які можуть виникнути за різних причин, й у тому числі через використання нових інформаційних технологій.

Окрім зазначеного, на нашу думку, слід враховувати, ступінь цифровізації компанії. Наприклад, треба відрізняти компанії, які мають цифровий ген з самого початку існування, від компаній виробників та постачальників послуг у секторі ІКТ, або від традиційних компаній, які використовують у своїй

діяльності певний набір інформаційних та комунікаційних технологій, що поліпшують роботу тих чи інших бізнес-процесів.

Якщо розглядати традиційну компанію, то можна взяти до уваги існуючу класифікацію підприємницьких ризиків [10; 11], де можна побачити, що вона певною мірою враховує деякі ризики, які виникають у процесі використання інформації та інформаційних технологій. Так, у табл. 1 можна бачити, що існують загрози та викликані ними ризики, з якими стикаються компанії у процесі використання інформації та інформаційних технологій, та які, певною мірою, співпадають з ризиками, які присутні в існуючій класифікації підприємницьких ризиків.

Таблиця 1

Складові інформаційних ризиків, які співпадають зі складовими підприємницького ризику

Характер прояву загроз	Зв'язок зі складовими підприємницького ризику
Знищення, вихід із ладу або перехід у неробочий стан технічних засобів внаслідок стихійних лих, втрата програмних засобів, інформаційних баз даних тощо.	Природно-кліматичний
Знищення, вихід із ладу або перехід у неробочий стан технічних засобів внаслідок аварій, втрата програмних засобів, інформаційних баз даних тощо. Проблеми з комунальними послугами (перебої у постачанні електроенергії тощо). Можлива наявність помилок у моделях, алгоритмах обробки інформації, програмах. Зниження достовірності, повноти та актуальності інформації на стадії її отримання та вводу в інформаційну систему. Різного роду помилки персоналу (адміністраторів, операціоністів та ін.	Техніко-технологічний
Перешкоджання функціонуванню інформаційної системи шляхом вводу, передачі, псування, порушення, зміни інформаційних даних. Крадіжка особистих та службових баз даних, шахрайство, пов'язане з їх використанням. Зловживання персоналу, пов'язані з незаконними діями щодо інформаційних ресурсів.	Кримінально-правовий

Джерело: складено з урахуванням даних у джерелах [10; 11]

Як видно у наведеній таблиці 1, коло зазначених загроз стосується перш за все техніко-технологічного та кримінально-правового ризиків. Тому, у процесі характеристики цих ризиків та наслідків їх прояву, слід ураховувати джерела та загрози, що безпосередньо пов'язані із використанням інформації та інформаційних технологій.

Там, де це можливо та доцільно, в системі класифікації підприємницьких ризиків ці ризики слід доповнити відповідними видовими ризиками, що дозволить розширити класифікацію без її руйнування.

Слід відзначити, що розглянуті у табл. 1 загрози пов'язані із безпосереднім впливом на інформаційну систему компанії. Проте, як показує аналіз, існує низка вагомих факторів, які впливають на кінцеві результати діяльності компанії, факторів ризику, пов'язаних із використанням інформації та інформаційних технологій, але які безпосередньо не впливають на інформаційну систему компанії.

До таких загроз можна віднести розповсюдження неправдивої інформації стосовно компанії, яка може негативно впливати на її імідж, а також матеріалів, що містять інформацію, яка характеризується негативним відношенням до компанії. Оскільки мова йде про будь-яке небажане інформаційне наповнення (контент) стосовно компанії, ризики, до яких призводить реалізація відповідних загроз можуть бути віднесені до так званих контентних ризиків компанії.

За змістом та спрямованістю така інформація може бути віднесена до неетичної, метою якої є негативний вплив на імідж компанії та нанесення їй збитків, шляхом маніпулювання свідомістю та діями інших акторів (партнерів, конкурентів, споживачів та ін.). Тому, з точки зору причинно-наслідкового підходу, такі дії за їх характером можуть бути віднесені до групи соціально-психологічних. Виходячи з складу ризиків, що включені до існуючої класифікації підприємницьких ризиків, найбільш обґрунтованим може бути розглядання контентних ризиків як складової соціальних ризиків. При цьому, з використанням правила побудови через рід та видову відмінність, можна надати їм таке визначення. *Контенті ризики* – це складова соціальних ризиків, яка визначає можливість незапланованої зміни кінцевого результату діяльності компанії внаслідок негативного впливу розповсюдження неправдивої інформації про неї та/або її співробітників.

Прагнення до здійснення цифрової трансформації та його реалізація природно призводить до розширення діяльності компанії у кіберпросторі, де інформація створюється, розповсюджується, обмінюється та споживається. Мережа як природне для інформації середовище, з одного боку, надає нові можливості для її учасників, з іншого – породжує коло небезпек, з якими може зустрітись компанія та її співробітники, інтегруючись у цифрові екосистеми. Високий рівень взаємозалежності елементів

посилюють вразливості системи та збільшують загрози для її учасників. Особливо це стосується компаній, які з самого початку свого існування мають середній чи високий рівень цифровізації (ІКТ-компанії, а також компанії, які реалізують свою діяльність на базі цифрових платформ).

Відомо, що існує низка факторів, наявність яких є необхідною умовою успішності будь-якої взаємодії. До них передусім слід віднести довіру, координацію дій, узгодженість стратегій, якість комунікацій між взаємодіючими підприємствами, здатність вирішення конфліктів шляхом спільного вирішення проблем тощо [12]. Їх відсутність породжує коло загроз для компаній, які здійснюють партнерську взаємодію у процесі реалізації сумісних підприємницьких проектів. Це може бути порушення компаніями партнерських угод, відсутність взаєморозуміння та єдності між представниками компаній-учасників партнерства, посилення залежності від інших компаній у бізнес-мережі, а також низка інших загроз, з якими можуть зіткнутися компанії у процесі інформаційно-мережевої взаємодії.

Слід зазначити, що партнерська взаємодія компаній, яка притаманна економічній діяльності, завжди була пов'язана з так званими партнерськими (інтеграційними) ризиками. Проте протягом значного часу вони суттєво не впливали на підприємницьку діяльність. Їх вплив у загальній системі підприємницьких ризиків був незначний. Ситуація для компаній змінилася внаслідок активізації процесів з цифрового перетворення, та, як наслідок, широкого розповсюдження інформаційно-мережевої взаємодії. Оскільки цифрова трансформація поступово охоплює й діяльність традиційних компаній, на нашу думку, партнерський ризик слід включити до класифікації підприємницького ризику як її самостійну складову. Для цього, як і у випадку контентного ризику, слід визначити місце партнерського ризику в системі класифікації, а також надати його визначення (дефініцію).

Оскільки вибір партнерів, як правило, є результатом свідомої діяльності компанії, то, з точки зору причинно-наслідкового підходу, небажані результати (ризики) такого вибору за їх характером можуть бути віднесені до групи організаційно-управлінських ризиків та її складової – селективного ризику, який є результатом недостатнього рівня обґрунтування управлінських рішень. У цьому випадку, з використанням правила побудови через рід та видову відмінність, партнерському ризику можна надати таке визначення. *Партнерський ризик* – це складова селективного ризику, яка визначає можливість незапланованої зміни кінцевого результату діяльності компанії внаслідок недостатнього обґрунтування рішень щодо вибору партнерів.

У свою чергу, якщо серед партнерів компанії є її конкуренти, необхідно враховувати наявність комплементарних відносин й виділяти відповідні ризики. Отже, *комплементарний ризик* – це складова партнерського ризику, яка визначає можливість незапланованої зміни кінцевого результату діяльності компанії внаслідок недостатнього обґрунтування рішень щодо вибору стратегії співпраці з компанією-конкурентом.

Слід також враховувати, що сучасна компанія є учасником різних соціальних екосистем (як у реальній, так і у цифровій (електронній) формах), де вона активно взаємодіє (співпрацює) з іншими учасниками для вирішення тих чи інших питань, як правило, без підписання партнерських угод. Тобто не кожна взаємодія (співпраця) передбачає партнерство. В умовах гіперзв'язності між суб'єктами господарювання, яка характерна для цифрової епохи, тенденція до взаємодії (співпраці) посилюється. Отже, для компаній, діяльність яких опосередковується інформаційно-мережевими відносинами, виникає необхідність брати до уваги й ризики, які виникають під час інтерактивних дій з іншими учасниками тої чи іншої соціальної екосистеми.

У цьому випадку, з використанням правила побудови через рід та видову відмінність [10; 11], можна сформулювати таке визначення: *інтерактивний ризик* – це складова соціальних ризиків, яка визначає можливість незапланованої зміни кінцевого результату діяльності компанії внаслідок негативного впливу небажаних (недобросовісних) дій інших учасників інтерактивності (взаємодії) у соціальній екосистемі або конфлікту інтересів, що унеможливлює співпрацю.

Слід зазначити, що можливі небезпеки, пов'язані з використанням інформації та інформаційних технологій, у явному або неявному вигляді присутні у більшості складових ризику підприємницької діяльності.

Разом з тим, як показують наші дослідження, коло небезпек, з якими може зустрітись компанія та її співробітники, здійснивши цифрову трансформацію й перейшовши на інформаційно-мережеву взаємодію (як внутрішню, так і зовнішню), значно ширше, ніж тільки питання втрати важливої інформації.

Отже, сучасний тренд «цифрової трансформації», з одного боку, відкриває компаніям світ нових можливостей й доступ до функціонування на новій технологічній основі. З іншого боку, чим більше компанія цифровізується, тим більше її діяльність стає залежною від правил гри у цифровому світі. Звідси, кожен з видів ризиків, які характерні для традиційного способу господарювання, наповнюється новим змістом. Також інформаційно-мережева взаємодія, інтеграція у кіберфізичні системи та інші процеси, які відбуваються в умовах нового технологічного устрою у XXI столітті, викликають нові джерела ризиків, які зовсім не були відомі раніше.

Висновки з проведеного дослідження. Як показує виконаний аналіз, сьогодні велика кількість компаній, обравши шлях «цифрової трансформації», здійснює свою діяльність через інформаційно-

мережеву взаємодію. У процесі дослідження визначено та обґрунтовано перелік загроз та викликані ними ризики, з якими стикаються компанії у процесі використання інформації та інформаційних технологій. Певною мірою вони співпадають з ризиками, які вже присутні в існуючій класифікації підприємницьких ризиків. За результатами дослідження особливостей діяльності сучасних компаній доповнено склад підприємницьких ризиків такими підвидами, як контентні, партнерські, комплементарні, інтерактивні ризики. Визначено їх взаємозв'язок з іншими ризиками компанії, місце в системі класифікації підприємницьких ризиків, надано визначення (дефініцію) цих ризиків. Подальші дослідження можуть бути пов'язані як з удосконаленням системи класифікації підприємницьких ризиків шляхом її розширення, так і з формуванням нової системи класифікації інформаційно-мережевих ризиків, різні види яких виникають по мірі того, як збільшується ефект «цифрової трансформації» у світі.

Виконані дослідження сприятимуть підвищенню якості аналізу ризиків сучасних компаній, а також можуть бути підґрунтям для вирішення у подальшому низки ключових проблем управління ризиками (передусім, кількісної оцінки та її використання при прийнятті управлінських рішень, зокрема у питанні превентивних мір та ін.).

Література

1. Rogers D. The Digital Transformation Playbook: Rethink Your Business for the Digital Age. New York: Columbia University Press, 2016. 296 p.

2. Venkatraman V. The Digital Matrix: New Rules for Business Transformation Through Technology. Vancouver, BC: LifeTree Media, 2017. 224 p.

3. Westerman G., Bonnet D., McAfee A. Leading Digital: Turning Technology into Business Transformation. Boston: Harvard Business Review Press, 2014. 256 p.

4. Herbert L. Digital Transformation. Build Your Organization's Future for the Innovation Age. London: Bloomsbury Business, 2017. 264 p.

5. Sacolick I. Driving Digital: The Leader's Guide to Business Transformation Through Technology. New York: AMACOM, 2017. 224 p.

6. Ahlemann F. How Digital Transformation Shapes Corporate IT: Ten Theses about the IT Organization of the Future. *Federated Conference on Computer Science and Information Systems*: Proceedings of the Federated Conference (Gdansk, Poland, 11–14 Sept. 2016). IEEE: 2016. pp. 3–4.

7. Reddy S., Reinartz W. Digital Transformation and Value Creation: Sea Change Ahead. *GfK MIR "Value in the Digital Era".* 2017. Vol. 9. No. 1. pp. 10–17.

8. Гранатуров В.М., Кораблінова І.А. Інформаційний ризик підприємства: щодо вирішення проблеми qui pro quo у визначенні поняття. *Інноваційна економіка*. 2017. № 5-6 (69). С. 199–206.

9. The Global Risks Report 2017. URL: http://www3.weforum.org/docs/GRR17_Report_web.pdf.. (дата звернення: 09.01.2018).

10. Гранатуров В. М., Литовченко І. В., Харічков С. К. Аналіз підприємницьких ризиків: проблеми визначення, класифікації та кількісної оцінки: монографія / за наук. ред. В. М. Гранатурова. Одеса: ІПРЕД НАН України, 2003. 164 с.

11. Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения: учебное пособие. 4-е изд. перераб. и доп. Москва: Дело и сервис, 2016. 288 с.

12. Mohr J., Spekman R. Characteristics of partnership success: partnership attributes, communication behavior, and conflict resolution techniques. *Strategic Management Journal.* 1994. № 15 (2). P.135–152.

References

1. Rogers, D. (2016), "The Digital Transformation Playbook: Rethink Your Business for the Digital Age", New York, Columbia University Press, 296 p.

2. Venkatraman, V. (2017), "The Digital Matrix: New Rules for Business Transformation Through Technology", Vancouver, BC, LifeTree Media, 224 p.

3. Westerman, G., Bonnet, D. and McAfee, A. (2014), "Leading Digital: Turning Technology into Business Transformation", Boston, Harvard Business Review Press, 256 p.

4. Herbert, L. (2017), "Digital Transformation. Build Your Organization's Future for the Innovation Age", London, Bloomsbury Business, 264 p.

5. Sacolick, I. (2017), "Driving Digital: The Leader's Guide to Business Transformation Through Technology", New York, AMACOM, 224 p.

6. Ahlemann, F. (2016), "How Digital Transformation Shapes Corporate IT: Ten Theses about the IT Organization of the Future*", Proceedings of the Federated Conference on Computer Science and Information Systems*, Gdansk, Poland, 11-14 Sept. 2016, IEEE, pp. 3–4.

7. Reddy, S. and Reinartz, W. (2017), "Digital Transformation and Value Creation: Sea Change Ahead" GfK MIR "Value in the Digital Era", Vol. 9, no. 1, pp. 10–17.

8. Granaturov, V.M. and Korablinova, I.A. (2017). "Information risk of the enterprise: to the solution for the problem qui pro quo in the definition of the concept", *Innovatsiina ekonomika,* no. 5-6 (69), pp. 199 – 206.
9. The Global Risks Report (2017), *The World Economic Forum*, available at: http://www3.weforum.org/docs/GRR17_Report_web.pdf (access date January 09, 2018).
10. Granaturov, V.M., Litovchenko, I.V. and Kharichkov, S.K. (2003), *Analiz pidpryiemnytskykh ryzykiv: problemy vyznachennia, klasyfikatsii ta kilkisnoi otsinky* [Analysis of business risks: problems of definition, classification and Quantitative assessment], monograph, for science. Ed. V. M. Granaturov., Institute of Market Problems and eco-ekon. research of Ukraine, Odessa, Ukraine, 164 p.
11. Granaturov, V.M. (2016), *Ekonomicheskiy risk: suschnost, metodyi izmereniya, puti snizheniya* [Economic risk: the essence, methods of measurement, ways to reduce], Delo i servis, Moscow, Russia, 288 p.
12. Mohr, J. and Spekman, R. (1994), "Characteristics of partnership success: partnership attributes, communication behavior, and conflict resolution techniques" *Strategic Management Journal*, no. 15 (2), pp. 135 –152.

Стаття надійшла до редакції 18.01.2018 р.

Рецензент: д.е.н., професор Одеської національної академії зв'язку ім. О.С. Попова В.М. Гранатуров

УДК 33.021 : 658 : 338.246

Меліхова Т.О.,
канд. екон. наук, доцент, доцент кафедри обліку, аналізу, оподаткування та аудиту
Запорізька державна інженерна академія

АНАЛІЗ НАЯВНИХ МЕТОДИК ОЦІНКИ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ДЛЯ ПРОВЕДЕННЯ СУЧАСНОЇ ДІАГНОСТИКИ ЙОГО ФІНАНСОВОГО СТАНУ

Melikhova T.O.,
cand.sc.(econ), assoc. prof., associate professor at the department of accounting, analysis, taxation and audit
Zaporizhzhia State Engineering Academy

ANALYSIS OF AVAILABLE METHODS FOR ASSESSING THE LEVEL OF ECONOMIC SECURITY OF AN ENTERPRISE FOR CONDUCTING MODERN DIAGNOSTICS OF ITS FINANCIAL CONDITION

Постановка проблеми. В сучасних умовах ефективне управління економічною безпекою підприємства є одним з головних завдань підприємства при здійсненні його господарської діяльності. Існуючі загрози внутрішнього та зовнішнього середовища впливають на рівень економічної безпеки. Тому існує об'єктивна необхідність у проведенні своєчасної оцінки економічної безпеки підприємства для виявлення та подолання наявний загроз та ризиків. Визначення рівня економічної безпеки України регламентується Наказом Міністерства економічного розвитку і торгівлі України від 29 жовтня 2013 року № 1277, який затверджує Методичні рекомендації щодо розрахунку рівня економічної безпеки України [1], але, на жаль, для підприємств відповідна методика розрахунку оцінки рівня економічної безпеки підприємств не розроблена на законодавчому рівні. Тому дослідження існуючих методик оцінки рівня економічної безпеки підприємства для проведення сучасної діагностики його фінансового стану з метою вибору методики, яка найчастіше використовується є актуальним.

Аналіз останніх досліджень і публікацій. Сутності і напрямкам забезпечення економічної безпеки України присвятили свої праці Шлемко В.Т., Бінько І.Ф. [8], Козаченко Г.В., Пономарев В.П., Ляшенко О.М. [9], Покропивний С.Ф. [11], Олейников Є.О. [12]. Дослідженням методик оцінки рівня економічної безпеки підприємства займаються Халіна В.Ю. [3], Нагорна І.І. [4], Ілляшенко О.В. [5; 13], Ковальов Д. [14], Мищенко С.М. [17]. В побудову концепції системи економічної безпеки підприємства