На наш погляд, перші три градації ймовірності небажаного кінця відповідають "нормальному", "розумному" ризику, за такого рівня ризику рекомендують приймати рішення про реалізацію інвестиційного проекту.

Висновки та перспективи подальших досліджень. Отже, призначення аналізу ризику – дати потенційним інвесторам необхідні дані для прийняття рішення про доцільність участі в проекті та передбачити заходи щодо захисту від можливих фінансових втрат.

Особливістю запропонованого підходу аналізу ризиків є використання вірогідних понять і статистичного аналізу. Це відповідає сучасним міжнародним стандартам і є дуже трудомістким процесом, який потребує пошуку та залучення різноманітної кількості інформації. Для реалізації цієї мети ми рекомендуємо залучати кваліфікованих консультантів, яким ставлять завдання і надають набір необхідної інформації. Така практика є розповсюдженою в західних країнах.

Перспективою подальших досліджень в цьому напрямку є пошук ефективних підходів мінімізації інвестиційних ризиків.

1. Гайдис Н.М. Інвестування. – Львів: Львів. банківський ін-т НБУ, 2002. – 271 с. 2. Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения: Учеб. пособие. – М.: Дело и Сервис, 2002. – 230 с. 3. Гуторов О.І. Інвестування. – Харків: Харк. нац. аграр. ун-т, 2003. – 293 с. 4. Мойсеєнко І.П. Інвестування. – К.: Знання, 2006. – 490 с. 5. Пересада А.А. Інвестиційний процес в Україні. – К.: Лібра, 1998. – 392 с. 6. Реверчук С.К., Реверчук Н.Й., Скоморович І.Г. Інвестологія: наука про інвестування. – К.: Атіка, 2001. – 264 с. 7. Устенко О.Л. Предпринимательские риски: основы теории, методология оценки и управление. – К.: Всеувито, 1996. – 160 с. 8. Шевчук В.Я., Рогожин П.С. Основи інвестиційної діяльності. – К.: Генеза, 1997. – 360 с. 9. Шляхи підвищення інвестиційної діяльності в Україні / Під заг. ред. В.Г. Федоренка. – Ніжин: Аспект-Поліграф, 2003. – 724 с.

УДК: 338.4

С.В. Князь, Н.Г. Георгіаді, Ю.О. Андріанов
Національний університет "Львівська політехніка"

ІНФОРМАЦІЙНА БЕЗПЕКА У СИСТЕМІ ФІНАНСОВОГО ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ІННОВАЦІЙНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

Розглядаються сутність поняття "інформаційна безпека", її види, функції і особливості формування у системі фінансового забезпечення розвитку інноваційної діяльності підприємства. Проведено уточнення, націлене на раціоналізацію управлінських дій, пов'язаних із розробкою і реалізацією механізмів захисту економічної інформації.

Essence of the concept «informative safety», its prospects, functions and features of forming in the system of the financial providing of development of innovative activity of enterprise is examined in the article. The conducted clarifications are aimed on rationalization of the administrative actions related to development and realization of mechanisms of defense of economic information.

Постановка проблеми та її зв'язок із важливими науковими та практичними завданнями. В умовах підвищення рівня інформатизації суб'єктів господарювання значна кількість

керівників підприємств все більше уваги приділяє заходам із забезпечення інформаційної безпеки підприємства. Ознайомлення із працями вітчизняних і зарубіжних науковців на цю тематику показало, що проблема формування інформаційної безпеки досліджена доволі фрагментарно. Ця робота розкриває сутність інформаційної безпеки у системі фінансового забезпечення (ФЗ) розвитку інноваційної діяльності підприємства (РІДП). Тема роботи відповідає тематиці госпдоговірних тем: "Удосконалення інформаційного забезпечення розробки бюджетів ВАТ "Маяк" № 1586; "Удосконалення системи управління та інформаційного забезпечення діяльності ДАКХ "Артем" № 1666, що підтверджує актуальність і своєчасність проведеного дослідження.

Цілі статті. Метою роботи є розкриття сутності поняття "інформаційна безпека", виділення її видів формулювання рекомендацій щодо покращання рівня інформаційної безпеки у системі фінансового забезпечення розвитку інноваційної діяльності підприємства.

Аналіз останніх досліджень і публікацій за проблемою. Ознайомлення із працями Баскервіля Р., Захеди Ф., Мельникова В., Рискіна М., Співака В., Лапусти М., Черніна А., Шиверського А., Ярочкіна В., Куркіна М., Глушка С., Шайкана А. та інших [1, 3, 6, 8–17] показало, що науковці, які займаються проблемами формування інформаційної безпеки підприємства, здебільшого приділяють увагу напрямкам забезпечення інформаційної безпеки, методам захисту інформації, способам протидії розголошенню конфіденційної інформації, технічним засобам захисту підприємства від несанкціонованого проникнення в інформаційну систему управління, особливостям аудиту рівня інформаційної безпеки підприємства тощо. Незважаючи на велику кількість наукових праць, окремі аспекти проблеми інформаційного забезпечення залишаються дискусійними, зокрема це стосується ідентифікування видів загроз, організаційного забезпечення процесу захисту управлінської інформації, а також механізмів мотивування працівників, відповідальних за формування і обслуговування систем інформаційного захисту підприємства.

Виклад основного матеріалу дослідження. Безпека – це стан, коли кому-небудь, чому-небудь ніщо не загрожує [1, с. 43]. Безпека підприємства – це стан захищеності життєво важливих інтересів підприємства, компанії від мафіозно-тіньових структур, нечесних конкурентів, а також здатність протистояти цим загрозам і реалізувати внутрішні цілі [5, с. 95]. Поняття «безпека» вживають тоді, коли ідентифіковано факт або ймовірність виникнення певної загрози. З огляду на це, види безпеки доцільно розглядати за видами загроз, які можуть виникнути для підприємства. Узагальнення позицій вітчизняних і зарубіжних науковців, а також власних досліджень дало змогу виділити такі види загроз для підприємств:

- втрата конкурентної позиції на ринку;
- втрата контролю над управлінням підприємством;
- втрата ресурсів;
- втрата здоров'я або життя власниками, керівниками, працівниками підприємства;
- втрата іміджу у бізнес-колах та певних преференцій через погіршення впливу діяльності підприємства на екологію, споживачів, партнерів по бізнесу тощо.

Причинами їх виникнення можуть бути:

1) дії або бездіяльність власників, керівників та працівників підприємства (бездіяльність, як правило, проявляється у навмисному або несвідомому ігноруванні факту витікання управлінської інформації. Витікання – це безконтрольний вихід конфіденційної інформації за межі організації або кола осіб, яким її було довірено [4, 7, 17]. Щодо дій власників, керівників та працівників підприємств, які стають причиною виникнення різноманітних небезпек, то здебільшого вони зводяться до розголошення конфіденційної управлінської інформації (зловмисні або необережні дії з конфіденційними відомостями, що призводять до ознайомлення з ними осіб, недопущених до цих відомостей [4, 7, 17]. Розголошення здійснюється у результаті як витоку інформації, так і в разі несанкціонованого доступу до неї (протиправне зумисне оволодіння конфіденційною управлінською інформацією особою або групою осіб, які не мають права доступу до неї));

2) цілеспрямовані дії конкурентів чи криміналітету (виникнення загроз внаслідок цілеспрямованих дій конкурентів чи криміналітету, як стверджують фахівці, можуть мати як легальний, так і нелегальний характер (таблиця)).

Легальні і нелегальні методи одержання інформації [7]

Легальні методи	Нелегальні методи
• аналіз інформації про підприємство, яка міститься у спеціалізованих відкритих джерелах • аналіз відомостей про підприємство, що передаються засобами масової інформації • "удавані" переговори про наймання на роботу працівників конкуруючих фірм • фактичний прийом на роботу працівників конкуруючих підприємств • "удавані" переговори з конкуруючим підприємством про наміри ділової співпраці • встановлення ділових зв'язків з партнерами підприємства-конкурента для непрямого одержання інформації з "третіх рук" • замасковані опитування працівників конкуруючих підприємств на конференціях, семінарах тощо • дослідження продукції конкуруючих підприємств за допомогою зворотного інжинірингу тощо	• викрадення документів, які містять конфіденційну інформацію • викрадення взірців нової продукції і матеріалів • шантажування працівників конкуруючого підприємства, що мають доступ до конфіденційної інформації • знімання і оптичні спостереження • несанкціоноване підключення до систем зв'язку і комп'ютерних мереж • засилання і вербування агентів тощо

Дії або бездіяльність власників та працівників підприємства, а також цілеспрямовані дії конкурентів чи криміналітету, як причини виникнення небезпеки, завжди пов'язані з інформацією, зокрема її видами, правами на отримання і використання, методами отримання і захисту інформації тощо. З огляду на це, є підстави стверджувати, що будь-який вид загроз має передусім інформаційний характер, а наслідком використання певної інформації є виникнення різноманітних небезпек, а саме: економіко-соціальної, в тому числі фінансової (втрата конкурентної позиції на ринку, втрата контролю над управлінням підприємством, втрата ресурсів, втрата іміджу у бізнес-колах та певних преференцій); життєдіяльності (втрата здоров'я або життя власниками, керівниками, працівниками підприємства). Враховуючи вищесказане, серед видів інформаційної безпеки необхідно виділяти економіко-соціальну безпеку та безпеку життєдіяльності.

Інформаційну безпеку в системі ФЗ РІДП доцільно розглянути як принцип ФЗ РІДП (сутність принципу полягає у тому, що управлінські рішення, які призводять до зміни джерел і структури формування та використання фінансових ресурсів для РІДП, вимагають врахування ймовірності реалізації загроз, зокрема економіко-соціального характеру, та загрози життєдіяльності власників, керівників і працівників підприємства), а також з позиції виконуваних функцій. Функцією інформаційної безпеки ФЗ РІДП є забезпечення захисту економіко-соціальних інтересів і життєдіяльності власників, керівників і працівників підприємства під час формування і використання фінансових ресурсів для РІДП. Ефективне виконання цієї функції можливе в тому випадку, якщо виконуються такі умови:

1) на підприємстві створено структурний підрозділ, який виявляє потенційні загрози для підприємства, розробляє і реалізовує заходи, націлені на усунення або послаблення їх дії;

2) керівником і працівниками структурного підрозділу, що займається інформаційною безпекою підприємства, є професіонали, які мають сучасні інформаційні технології, інформацію про новітні засоби забезпечення безпеки;

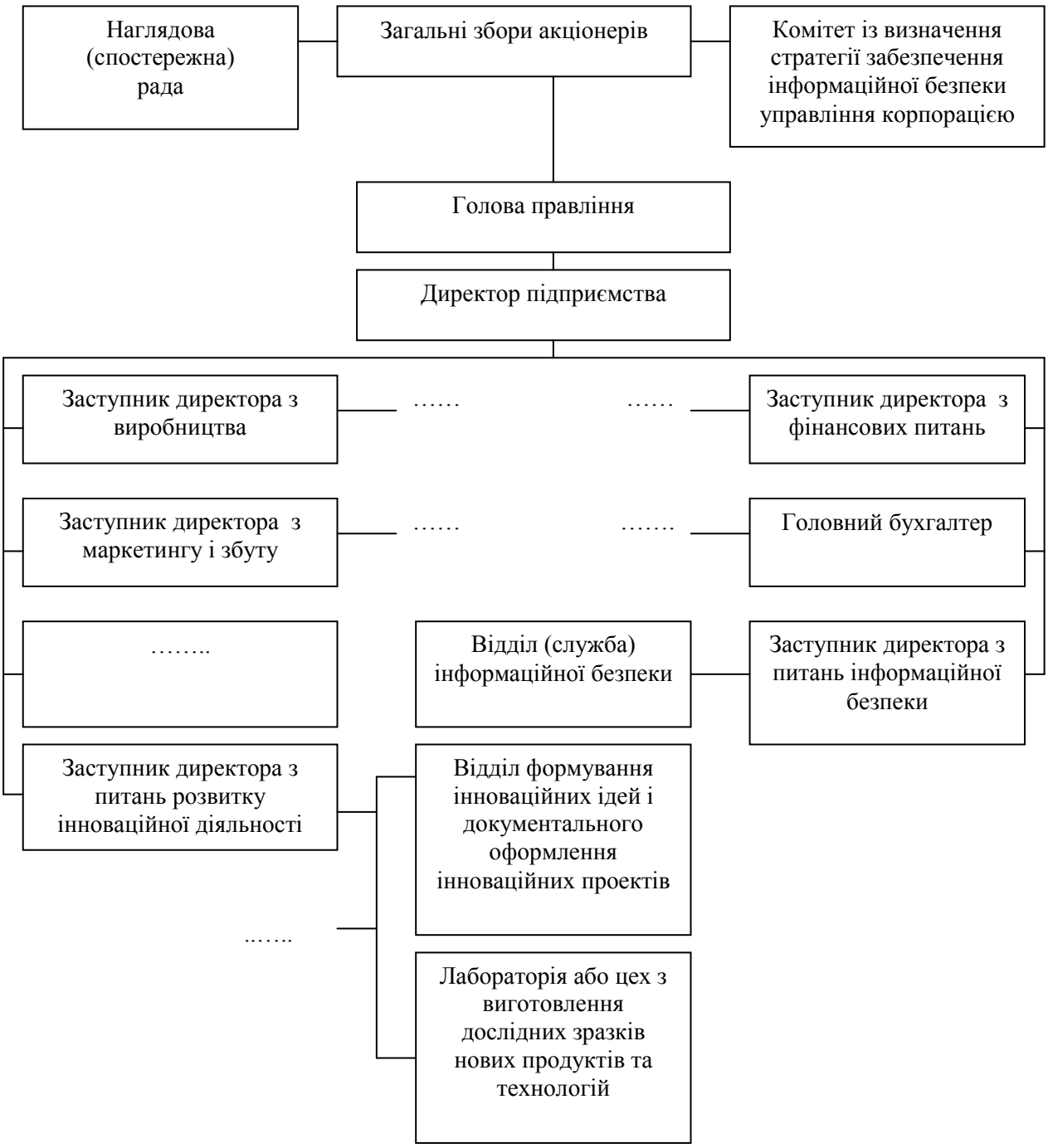
3) керівники і працівники відділу чи служби інформаційної безпеки підприємства зацікавлені у своєчасності і повноті виконання покладених на них обов'язків;

4) є наявною концепція інформаційної безпеки підприємства, інструкції і методичні рекомендації щодо правил отримання, зберігання, оброблення і використання управлінської інформації;

5) з користувачами управлінської інформації постійно проводиться робота на предмет їх інформування про стан і правила поводження з інформацією, а також на предмет посилення їх зацікавленості і відповідальності за дотриманням встановлених правил;

6) на підприємстві створено цільовий фонд грошових коштів для підвищення рівня інформаційної освіти управлінських працівників і заміни використовуваних інформаційних технологій та інших засобів безпеки на більш ефективні.

На рисунку показано місце структурного підрозділу із забезпечення інформаційної безпеки підприємства в організаційній структурі управління підприємством на прикладі корпорації.



Фрагмент організаційної структури управління підприємством

Як бачимо, в організаційній структурі управління корпорацією доцільно виділяти три рівні управління інформаційною безпекою підприємства. На вищому рівні доцільно створювати комітет із визначення стратегії забезпечення інформаційної безпеки управління корпорацією, функціями якого є формування концепції інформаційної безпеки корпорації і стратегії її забезпечення. Рішення цього комітету повинні бути обов'язковими до виконання усіма структурними підрозділами управління корпорацією. З огляду на це, цей комітет повинен формуватись з представників загальних зборів акціонерів, а його рішення (концепція і стратегія інформаційної безпеки) варто ухвалювати на загальних зборах акціонерів. Середнім рівнем управління інформаційною безпекою, як зрозуміло з рисунка, є заступник директора з питань інформаційної безпеки. Його функцією є розробляти механізми забезпечення інформаційної безпеки підприємства відповідно до концепції і стратегії інформаційної безпеки, які розроблені Комітетом із визначення стратегії забезпечення інформаційної безпеки управління корпорацією, та здійснювати управління процесом впровадження і функціонування цього механізму. Заступник директора з питань інформаційної безпеки здійснює лінійне керівництво відділом (службою) інформаційної безпеки, який є низовим рівнем управління інформаційною безпекою підприємства. Функцією цього підрозділу є впровадження в дію механізмів забезпечення інформаційної безпеки, розроблених заступником директора з питань інформаційної безпеки.

Наведений фрагмент організаційної структури управління підприємством побудовано на засадах лінійних зв'язків між структурними підрозділами організації, проте очевидним є те, що функціонально заступник директора з питань інформаційної безпеки та відділ (служба) інформаційної безпеки є пов'язаними з іншими структурними підрозділами. Так, зв'язки цих підрозділів з заступником директора з питань РІДП та підзвітними йому підрозділами відбувається на предмет прогнозування впливу інновацій на рівень інформаційної безпеки підприємства, виявлення ймовірних загроз для підприємства під час залучення інвесторів та кредиторів до реалізації інновацій, матеріально-технічного постачання процесу формування і реалізації інновацій тощо.

Проведені дослідження дають змогу стверджувати, що важливим чинником, який впливає на рівень інформаційної безпеки як підприємства загалом, так і безпеки РІДП зокрема, є зацікавленість управлінських працівників в економічному розвитку підприємства (сукупність стійких і тимчасових кількісних і якісних змін результативних ознак досліджуваного об'єкта. Виявити стійку зміну результативних ознак означає ідентифікувати факт наявності або відсутності економічного розвитку досліджуваного об'єкта. Своєю чергою, виявлення тимчасової зміни результативних ознак означає додатково охарактеризувати конкретний період або момент економічного розвитку підприємства. Він може свідчити про тимчасове зростання або зниження значення результативних ознак, що загалом не має істотного впливу на виявлені довготривалі тенденції. Поряд з цим тимчасові зміни необхідно виявляти і аналізувати з метою пошуку причини погіршення значень показників діяльності підприємства та розроблення заходів щодо їх усунення у майбутньому. Виявлення факту стійкої зміни результативних ознак характеризує також потенціал економічного розвитку підприємства, його можливості щодо реалізації очікуваних якісних та кількісних змін результативних ознак. Результативними ознаками потрібно вважати показники економічного розвитку підприємства [7]).

Ознайомлення із матеріалами підприємств показало, що на тих підприємствах, де добре розвинута система мотивування управлінських працівників, випадки несанкціонованого витоку управлінської інформації, розголошення та несанкціонований доступ до управлінської інформації значно рідше зустрічаються, ніж на підприємствах, де така система розвинута слабко або з певних причин є недієвою. З огляду на це, серед завдань, які необхідно виконати для забезпечення інформаційної безпеки ФЗ РІДП, доцільно виділяти створення системи мотивування працівників, зокрема посилення їх зацікавленості в економічному розвитку підприємства.

Висновки і перспективи подальших досліджень:

- формування і використання ФЗ РІДП доцільно здійснювати із врахуванням його впливу на рівень безпеки підприємства;

- поняття “безпека” вживають у тому випадку, якщо ідентифіковано факт або ймовірність виникнення певної загрози, а саме: втрати конкурентної позиції на ринку; втрати контролю над управляннням підприємством; втрати ресурсів; втрати здоров’я або життя власниками та працівниками підприємства; втрати іміджу у бізнес-колах та певних преференцій через погіршення впливу діяльності підприємства на екологію, споживачів партнерів з бізнесу тощо;
- причинами виникнення загроз можуть бути: дії або бездіяльність власників та працівників підприємства; цілеспрямовані дії конкурентів чи криміналітету;
- будь-який вид загроз носить передусім інформаційний характер, а наслідком використання певної інформації є виникнення різноманітних небезпек, а саме: економіко-соціальної, в тому числі фінансової; життєдіяльності працівників;
- функцією інформаційної безпеки ФЗ РІДП є забезпечення захисту економіко-соціальних інтересів і життєдіяльності власників і працівників підприємства під час формування і використання фінансових ресурсів для РІДП.

Подальші дослідження необхідно здійснювати у напрямку формалізації методів формування систем захисту економічної інформації та розроблення механізмів їх оптимального комбінування.

1. Баскервиль Р. Защита информации и ИТ/С // Информационные технологии в бизнессе: Энциклопедия / Под ред. М. Желены. – СПб.: Питер, 2002. – С. 742–751. 2. Великий тлумачний словник сучасної української мови / Уклад. і голов. ред. В.Т. Бусел. – К.: Ірпінь: ВТФ “Перун”, 2003. – С. 386–1087. 3. Гушко С.В., Шайкан А.В. Управлінські інформаційні системи: Навч. посібник. – Львів: Магнолія плюс, 2006. – 320 с. 4. Георгіаді Н.Г., Князь С.В. Інформаційна безпека в системі управління економічним розвитком підприємства // Теорії мікро-макроекономіки: Зб. наук. пр. проф.-викл. складу і асп. – К.: Академія муніципального управління, 2006. – Вип. 25. – С. 191–196. 5. Економічна енциклопедія: У 3 т. Т. 1 – К.: Вид. центр “Академія”, 2000. – 864 с. 6. Захеди Ф. Индустрия информации и знаний // Информационные технологии в бизнессе: Энциклопедия / Под ред. М. Желены. – СПб.: Питер, 2002. – С. 104–128. 7. Кузьмін О.Є., Георгіаді Н.Г. Формування і використання інформаційної системи управління економічним розвитком підприємства: Монографія. – Львів: Вид-во Нац. ун-ту “Львівська політехніка”, 2006. – 368 с. 8. Как преуспеть на ниве аутсорсинга? // Компьютерное обозрение. – 2006. – № 42. – С. 74–75. 9. Куркін М.В. Механізм управління економічною безпекою розвитку підприємства: Автореф. дис. …д-ра екон. наук. – Харків, 2006. – 36 с. 10 Мельников В.В. Защита информации в компьютерных сетях. – М.: Финансы и статистика. Электронинформ, 1997. – 368 с. 11. Рыскин М.В. Обработка деловой информации. – М.: Статистика, 1986. – 128 с. 12. Спивак В.А. Современные бізнес-коммуникации. – СПб.: Питер, 2002. – 448 с. 13. Справочник директора предприятия / Под ред. проф. М.Г. Лапусты. – М.: ИНФРА-М, 2003. – 832 с. 14. Чернин А.Э. Системы управления документацией // Мир ПК. – 1992. – № 6. – С. 83–92. 15. Что значит быть лидером // COMPUTERWORLD/УКРАИНА. Информ.-аналитич. еженедельник. – 2005. – № 3–4 (485). – С. 27. 16. Шиверский А.А. Защита информации: проблемы теории и практики. – М.: Юрист, 1996. 17. Ярочкин В.И. Информационная безопасность: Учеб. для студентов вузов. – М.: Академический Проект; Фонд “Мир”, 2003. – 640 с.