УДК 657.1:004.056.5

Боримська К.П., к.е.н., доц.
Житомирський державний технологічний університет

РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В СПЕКТРІ СИСТЕМИ БУХГАЛТЕРСЬКОГО ОБЛІКУ

Досліджено місце інформаційної складової бухгалтерського обліку в системі інформаційної безпеки підприємства

Ключові слова: *інформаційна безпека, бухгалтерська інформація, ризики діяльності підприємства*

Постановка проблеми. Управління сучасним підприємством нерозривно пов'язане з реалізацією концепції інформаційної безпеки. В умовах стрімкого розвитку інформаційно-комп'ютерних технологій й використання переваг мережі Інтернет, не лише полегшується доступ до різних інформаційних ресурсів, а й збільшуються обсяги поширення інформації, забороненої для розголошення, зі статусом комерційної й таємної, зростають витрати суб'єктів господарювання від витоку такої інформації, від зламу інформаційних мереж, рейдерсько-хакерських дій, що знижує не лише рівень прибутковості підприємства, але й надійності й соціальної значущості бізнесу.

Глобальне дослідження аналітичного центру Info Watch, проведене доц. С.В. Кавуном [55], засвідчило, що за 2011-2012 рр. було зафіксовано 249 інцидентів витоку інформації з обмеженим доступом (витоки охопили більше 100 млн. людей). 29 % витоків інформації здійснюється через мережу (в т.ч. Інтернет), 25 % – через мобільні носії інформації, 14 % – не встановлено, 12 % – через стаціонарний комп'ютер або диск, 9 % – через паперовий документ, по 4 % – через електронну пошту, факс та інше, 3 % – через архівну копію. Для випадкових витоків мобільні носії інформації (CD, DVD, флеш-носії) випереджають витоки через мережу Інтернет (30 % проти 24 %). При цьому за даними світової статистики, втрата тільки 20 % інформації веде до руйнування 65 % підприємств [4].

Вищепредставлені канали витоку інформації реалізуються через такі заходи несанкціонованого доступу: підслуховування, візуальне спостереження, розкрадання, копіювання, підробка, незаконне підключення, перехоплення, фотографування. Тобто із розвитком науково-технічного прогресу не лише удосконалюються засоби матеріального забезпечення ведення бізнесу, але й розширюються технології витоку інформації, як важливого стратегічного ресурсу в конкурентній боротьбі. Оцінюючи зростання попиту на якісну інформацію, слід відзначити, що вона стає визначальним компонентом – активом будь-якої фірми, її стратегічного розвитку, найбільшу вигоду з яких уміють отримувати лідери ринку, знижуючи цим ступінь ризиків здійснення інвестицій [5].

Піратство у сфері інтелектуальної власності щодо програмного забезпечення (ПЗ) займає третє місце в світі з прибутковості після розповсюдження наркотиків і зброї, що і робить його одним з найбільш небезпечних видів комп'ютерних злочинів, включених в міжнародну класифікацію (вид QR – незаконне копіювання) [42; 8].

У повідомленнях ЗМІ часто з'являється інформація про те, що у різних країнах світу все більше виникає фірм, які пропонують послуги бізнес-шпигунства. Зокрема, в Росії вартість таких послуг може коливатися від 500 до 15 тис. доларів [13]. Переважно клієнтів подібних фірм цікавлять відомості про роботу підприємства-конкурента, його плани, оригінальні ідеї, організація виробничого процесу тощо.

За даними видання "Інформаційна безпека", на початку 2010 року офіс компанії "PricewaterhouseCoopers" (PwC) у Чикаго повідомив про виток 77 тис. персональних даних на державних службовців штату Аляска [49]. Причому повідомлення було здійснено не відразу, а тільки через два місяці після встановлення витоку. Досить цікаві дані були отримані за результатами опитування "Harris Interactive", які були опубліковані у серпні 2010 року [23]. За цими показниками кожен п'ятий співробітник організації здійснює крадіжку конфіденційної інформації. Аналітичний центр компанії "InfoWatch" повідомив, що у грудні 2010 року один із банків Нью-Йорка порушив у суді справу стосовно колишніх працівників банку за крадіжку відомостей, які містили інформацію з обмеженим доступом. Як зазначалось у позові, четверо колишніх працівників банку напередодні свого звільнення скопіювали захищену базу даних. У відомостях, крім комерційної таємниці, містились персональні дані (імена, адреси, телефонні номери, адреси електронних скриньок тощо) клієнтів. Звільнення працівників було пов'язано із запрошенням на роботу до іншої фінансової компанії.

Відповідно до результатів дослідження компанії "PricewaterhouseCoopers" (PwC) 40 % організацій навіть не знають справжньої кількості інцидентів щодо витоків їх інформації з обмеженим доступом за минулий рік [20; 50].

За таких умов постає необхідність розробки методичних аспектів побудови адекватної системи захисту інформації на підприємстві, які сприяють реалізації комплексної системи інформаційної безпеки підприємства. В умовах жорсткої конкурентної боротьби, виснаження природних ресурсів, розвитку інформаційно-інноваційних процесів на підприємстві, переходу до постіндустріального суспільства інформація стає затребуваною все більше, адже ускладнюються умови прийняття рішень, їх наслідки та ефективність, що обумовлює розгляд системи бухгалтерського обліку, яка є основним джерелом формування й представлення такої інформації, в системі управління підприємством.

Аналіз результатів останніх досліджень і публікацій. Окремим аспектам проблеми забезпеченості належного рівня інформаційної безпеки приділяється увага такими зарубіжними та вітчизняними ученими, як: С. Бармен [3], Н.В. Ващенко [14], В.А. Галатенко [9], Л.І. Донець [14], С.М. Ілляшенко [18], Д. Ковальов [24], А.В. Козаченко, В.П. Пономарьов, А.Н. Ляшенко [25], Т.С. Клєбанова [22], О.Я. Кравчук [26], О. Крилова [27], М.В. Куркін [28], Д.М. Прокоф'єва [35], Є.А. Олєйников [51], Н.Й. Реверчук [38], О.П. Савва [39]. Існує ряд міжнародних стандартів, методик та інших документів, що регламентують питання створювання системи інформаційної безпеки і безпечного використання інформаційних технологій розроблено [53; 54].

Проблеми обліків-аналітичного забезпечення управління діяльністю підприємства знайшли відображення в працях: І.А. Аврової [1], П.С. Безруких, В.Б. Івашкевича, Н.П. Кондракова, В.Д. Новодворського [7], Ф.Ф. Бутинця [19], В.М. Добровського, Л.В. Гнилицької [10; 11; 12], Є. Кириченка [21], Н.П. Кондракова, Т.К. Киселева [47], Ю.А. Мішина [29], Л.В. Нападовської [48], В.Ф. Палія, Я.В. Соколова [2], М.С. Пушкаря [36; 37], В.В. Сопка [43], Т. Стоуна [45], Р.П. Юзва [52] та ін.

Метою дослідження є розкриття ролі інформаційної системи бухгалтерського обліку у вирішенні проблем інформаційної безпеки підприємства, насамперед, щодо формування інформаційних ресурсів з підвищеним рівнем їх оперативності, вірогідності й мінімальним показником ризиковості.

Викладення основного матеріалу. Значення інформації для економічного життя значно зростає в умовах становлення постіндустріального суспільства, фундаментом якого є інформаційна економіка – особливий тип економіки, який характеризується пануванням інформаційної парадигми. Витоки "інформаційної економіки" можна прослідкувати, вивчаючи розвиток моделей раціонального вибору з врахуванням

невизначеності. В таких моделях, якщо процес прийняття рішень агентом задовольняє певні фундаментальні логічні аксіоми, то таку поведінку можна назвати максимізацією його очікуваної корисності: якщо суб'єктивна імовірність відома, то особа, яка приймає рішення, використовує знання для максимізації власної функції корисності [40, с. 305]. Вчені говорять про інтелектуалізацію економіки, про економіку що базується на знаннях (економіку знань), про інтелектуальну або навіть ідеальну систему обліку [36; 37].

Інформаційні системи в сучасних умовах перетворюються на інструмент підвищення ефективності управління й створення нових конкурентних переваг і тому займають не останнє місце у всіх галузях бізнесу. Невід'ємною частиною будь-якого підприємства становляться інформаційні системи. Все більше критично важливої для підприємства інформації зберігається і обробляється в комп'ютерних системах. Разом з цим, поступово підвищується і складність інформаційних систем, що само стає фактором небезпеки.

Дослідження довели, що у процесі безсистемного розвитку інформаційні системи перестають забезпечувати необхідний рівень продуктивності, в цілому не функціонують як єдиний комплекс, оскільки не всі додатки інтегровані, оперативність внесення змін й реалізація нових функцій, які мають відповідати новим вимогам, значно нижчі за критичну, відсутня єдина система інформаційної безпеки.

Досить слушними вважаємо зауваження О.М. Степанової [44] щодо того, що до недавнього часу саме поняття інформаційної безпеки асоціювалося виключно з державними підприємствам, а на сьогодні експансивний характер автоматизації приватного бізнесу, введення поняття "комерційна таємниця" і жорстка конкуренція у сфері виробництва примушують керівників підприємств різного масштабу все більше замислюватися над забезпеченням безпечної експлуатації інформаційних ресурсів в умовах їхнього розвитку.

Поняття інформації в загальному вигляді містить [16] ст.1 закону України "Про інформацію": Відповідно до ст. 30 цього Закону інформація за обмеженим доступом поділяється на конфіденційну та таємну. З приводу складу злочину, що розглядається (підприємницького шпигунства), інтерес становитиме власне конфіденційна інформація.

В Україні не створено спеціального законодавства з приводу питань комерційної таємниці, існує лише підзаконний акт (окрім загального законодавства про інформацію) – Постанова Кабінету Міністрів України від 09.08.1993 р. "Про перелік відомостей, що не становлять комерційної таємниці" [17]. Україна є учасницею 18 багатосторонніх міжнародних договорів, що діють у цій сфері. Правовідносини, пов'язані з правовою охороною інтелектуальної власності, регулюють також близько 100 підзаконних нормативних актів [34]. Питання щодо змісту інформації, яка становить комерційну таємницю, є дискусійним. Це, зокрема, стосується співвідношення понять комерційної таємниці та інтелектуальної власності. Інформація може бути не лише об'єктом права власності, а й права інтелектуальної власності.

Інформація на сьогоднішній день є комерційним об'єктом, а, отже, потребує захисту. На відміну від природних ресурсів, що виснажуються, інформація не зникає при використанні, а змістовно тільки збагачується. Тому інформація має унікальну якість – бути індикатором будь-якого соціального процесу й суспільного життя в цілому [6, с. 85].

Погоджуємося з твердженням Я.М. Білокомірової [4], що інформаційна безпека заснована не тільки на захисті власної інформації, у тому числі конфіденційної, але й проводить ділову розвідку, інформаційно-аналітичну роботу із зовнішніми й внутрішніми суб'єктами. Інформацію можна продати, купити, імпортувати, фальсифікувати, украсти і т. д.

Інформація, якою обмінюється людина через машину з іншою людиною чи машиною, може бути важливою і, отже, є предметом захисту. Однак захисту підлягає не будь-яка інформація, а тільки та, котра має ціну. Цінною ж стає та інформація, володіння якою дасть змогу її дійсному чи потенційному власнику одержати який-небудь виграш: моральний, матеріальний, політичний і т. д. Отже, на перший план виходить необхідність і проблема захисту інформації, що становить комерційну таємницю.

Для захисту інформації, що становить комерційну таємницю, на підприємстві може бути створена служба безпеки, особливості функціонування якої визначаються тим, що на неї покладені обов'язки з організації режимів конфіденційного діловодства; організації допуску співробітників і сторонніх осіб до конфіденційної інформації; організації зберігання, обліку і знищення носіїв конфіденційної інформації; виявлення каналів можливого витоку інформації, їхня нейтралізація; проведення профілактичної роботи і службових розслідувань; протидії технічним засобам промислового шпигунства; проведення спеціальних акцій, спрямованих на створення сприятливого середовища і нормального функціонування власного підприємства; зв'язку зі службами безпеки інших фірм і державних структур; взаємозв'язку із засобами масової інформації [35].

Для забезпечення інформаційної безпеки підприємства у складі служби безпеки можуть бути організовані підрозділи конкурентної (ділової) розвідки, контррозвідки та інформаційно-аналітичної служби. Кожна з цих служб виконує певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової економічної безпеки. До таких належать: 1) збирання всіх видів інформації, що стосується діяльності того чи того суб'єкта господарювання; 2) аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів (систематизації, безперервності надходження, всебічного характеру аналітичних процесів) і методів (локальних із специфічних проблем, загальнокорпоративних) організації робіт; 3) прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів на підприємстві, в країні та у світі для конкретної сфери бізнесу, а також показників, яких необхідно досягти суб'єкту господарювання; 4) оцінка рівня економічної безпеки за кожною складовою окремо та в комплексі, розроблення рекомендацій щодо підвищення цього рівня на конкретному підприємстві; 5) інші види діяльності з розробки інформаційної складової економічної безпеки (зв'язок із громадськістю, формування сприятливого іміджу фірми, захист конфіденційної інформації) [15].

Також не менш важливим є захист інформації, яка міститься на машинних носіях. Сюди входить захист конфіденційної інформації, а також захист самих машинних носіїв інформації.

За таких умов зростає значення побудови системи інформаційної безпеки підприємства, максимально налаштованої на особливості управління інформаційними потоками сучасних суб'єктів господарювання. Під інформаційними потоками автори розуміють сукупність умов формування, систематизації, руху й використання економічної інформації на мікро- та макрорівнях, яка в цілому в процесі функціонування покликана забезпечити безпеку національної економіки. Концентруючись на мікрорівні, під управлінням інформаційними потоками розуміємо процес реалізації своїх функцій взаємопов'язаних дій (починаючи з визначення потреби в інформації, подальшої її збору, систематизації, руху й використання, та завершуючи зворотнім зв'язком – відтворенням та обміном інформацією). На кожному етапі такого процесу можливі об'єктивні й суб'єктивні втрати інформаційних потоків.

Проф. І.В. Пенькова та асп. О.І. Левченко [31] до неминучих втрат інформаційних потоків на рівні держави відносять: недосконалість законодавчої бази, низька швидкість і недосконалість ІК-мереж, висока вартість інформації на міжнародних сайтах; на рівні регіону – відсутність певних повноважень у місцевих органів влади, несвоєчасність інформування регіонів про зміни у законах, висока вартість підводу ІК-мереж; на рівні підприємства – висока вартість ліцензійного програмного забезпечення, несвоєчасність інформування державними інститутами,

висока вартість ІК-мереж і комп'ютерного обладнання. Втрати від неефективної діяльності суб'єктів інформаційних потоків (суб'єктивних) дослідники позиціонують наступні: на макрорівні – неузгодженість дій державних інститутів, високі податки, недостатність фінансування НДДКР; на мезорівні – неузгодженість дій інститутів влади різних рівнів, неініціативність керівників, відсутність доступу до ІК-мереж; на мікрорівні – неналагодженість каналів зв'язку та комунікацій, трансакційні витрати неефективних управлінських рішень, несвоєчасна реакція на зміни зовнішнього середовища.

Отже, робота над концепцією інформаційної безпеки України спрямована на систематизацію питань, які поєднані в проблему забезпечення інформаційної безпеки країни, на визначення методів і засобів захисту життєво важливих інтересів особистості, суспільства, держави в інформаційній сфері, на створення засад для формування державної політики інформаційної безпеки, розвитку інформаційного простору країни [32, С. 800-801].

Для забезпечення інформаційної безпеки підприємницької діяльності необхідна ефективна державна політика, яка передбачає створення загальнодержавної системи інформаційної безпеки [39; 46]. Обов'язковою умовою створення цієї системи є розробка відповідної нормативної бази, розвиток та вдосконалення системи сертифікації систем та засобів захисту інформації, програмних та апаратно-програмних засобів, відтворення системи органів контролю за станом інформаційної безпеки на підприємствах та контроль за їх діяльністю з боку держави; створення сприятливих умов для підприємств, організацій та налагодження виробництва вітчизняних засобів захисту інформації, створення системи підготовки наукових кадрів в галузі захисту інформації; вдосконалення системи підготовки та перепідготовки кадрів для роботи в сфері інформаційної безпеки; врегулювання відносин в галузі використання Internet, створення системи інформаційної безпеки, яка спроможна забезпечити належний рівень її захищеності в умовах постійного удосконалення можливостей технічних розвідок та засобів ведення інформаційних війн, ведення державного контролю за розробкою вітчизняних та ввезення імпортних засобів обчислювальної техніки та ін., на що наголошує Я.М. Білокомірова [4].

Для створення ефективної системи інформаційної безпеки підприємницької діяльності, на думку Я.М. Білокомірової [4], необхідно: 1. Здійснювати контроль над ймовірними каналами витоку інформації на підприємстві; 2. Здійснювати моніторинг доступу співробітників до корпоративних інформаційних ресурсів; 3. Зберігати архів операцій з документами; 4. Виявляти у вихідному потоці електронної пошти повідомлень, які можуть передбачати загрозу витоку конфіденційної інформації; 5. Виявляти у вихідному HTTP-потоці даних, які можуть передбачати загрозу витоку конфіденційної інформації; 6. Контролювати використання мобільних пристроїв зберігання інформації, пристроїв передачі інформації і комунікативних портів; 7. Архівувати поштову кореспонденцію; 8. Здійснювати моніторинг на рівні файлових операцій; 9. Контроль за діяльністю співробітників, доступу та використання ними лише тієї інформації, яка потрібна для роботи; 10. Правильний підбір кадрів, застосування матеріальних та моральних стимулів, створення сприятливого соціально-психологічного клімату всередині організації, створення можливостей для професійного росту, зниження плинності кадрів, формування "фірмового патріотизму". Однак лише своєчасне та комплексне виконання усих цих завдань може призвести до бажаного результату.

На важливість комплексної структури побудови забезпечення інформаційної безпеки на всіх етапах життєвого циклу інформаційної системи наголошує і О.М. Степанова [44]. Наприклад, обов'язкове використання деяких засобів ідентифікації і аутентифікації об'єктів та суб'єктів, засобів резервного копіювання, антивірусного контролю і т.д. Режим інформаційної безпеки в подібних системах забезпечується:

– на адміністративному рівні – політикою безпеки організації, в якій сформульовані цілі у сфері інформаційної безпеки і способи їхнього досягнення; на процедурному рівні – шляхом розробки і виконання розділів інструкцій для персоналу, присвячених інформаційній безпеці, а також заходами фізичного захисту;

– на програмно-технічному рівні – вживанням апробованих і сертифікованих рішень, стандартного набору контрзаходів: резервного копіювання, антивірусного і парольного захисту, міжмережевих екранів, шифрування даних і т.д.

Отже, режим інформаційної безпеки на рівні підприємства має охоплювати як організаційні (розробка положення про інформаційну безпеку з визначенням цілей інформаційної безпеки та способів їх досягнення, закріплення рівнів доступу до інформації, в тому числі, з обмеженим доступом (конфіденційної), порядок видачі особистих кодів, карток, паролів доступу до певних ділянок та носіїв інформації, контроль за входом до системи та складання звіту робочого часу, ознайомлення їх з правилами поведінки з конфіденційною інформацією та відповідальністю за її санкціоноване та несанкціоноване розголошення персоналом підприємства), так і програмно-технічні складові (обов'язкове використання засобів ідентифікації і аутентифікації об'єктів та суб'єктів, засобів резервного копіювання, антивірусного та парольного захисту, міжмережевих екранів, шифрування даних і т.д.). Заходи із забезпечення інформаційної безпеки, з одного боку, мають бути спрямовані на охорону конфіденційної інформації (зокрема, усунення "жучків", запобігання несанкціонованому доступу до локальних комп'ютерних мереж тощо), з іншого – забезпечувати пошук даних про конкурентів, партнерів, контрагентів, які слугують запобіганню виникненню можливих ризикових ситуацій в діяльності суб'єкта господарювання, викликаних недобросовісною конкуренцією, рейдерськими схемами захоплення бізнесу тощо.

Крім важливості режимної складової в концепції інформаційної безпеки, все ж таки визначальну роль відіграє налагоджена система управління інформаційними потоками сучасних суб'єктів господарювання, основна частина яких формується в системі бухгалтерського обліку, яка, з точки зору забезпечення належного рівня інформаційної безпеки підприємства, виконує подвійну роль. З одного боку – бухгалтерська інформація є основним достовірним, документально підтвердженим, джерелом даних для проведення розрахунків з контрагентами, визначення резервів діяльності підприємства, достатності коштів для придбання програмно-технічних заходів інформаційного захисту тощо. З іншого боку, сама підсистема бухгалтерського обліку в системі управління є фактором загроз інформаційній безпеці суб'єкта господарювання, адже реєстрація в обліку недостовірної інформації, маніпуляції, приховування інформації й шахрайство зі сторони керівництва та головного бухгалтера, отримання доступу до облікової інформації сторонніх осіб, значно знижує рівень захищеності підприємства від можливих законних та незаконних дій суб'єктів, як внутрішнього, так і зовнішнього середовища діяльності підприємства.

Так, згідно з опитуванням 250 осіб-представників 100 промислових підприємств, які входять до Українського союзу промисловців та підприємців, проведеним Л.В. Гнилицькою [11], найбільша кількість респондентів (власників та менеджерів) серед загроз, які пов'язані з кругообігом обліково-аналітичної інформації та справляють найсуттєвіший вплив на стан економічної безпеки виробничого підприємства, виділили низьку пристосованість обліково-аналітичних даних до потреб економічної безпеки (30 % власників та 23 % менеджерів) і недостовірність інформації, представленої у звітності контрагентів (27 % власників та 35 % менеджерів). На думку дослідниці, облікова інформація і, зокрема, бухгалтерська інформація як її основна складова, виступаючи внутрішнім ресурсом забезпечення економічної безпеки, за певних

обставин сама може нести суттєві ризики (загрози) діяльності підприємства. Це викликано тим, що формування бухгалтерських даних відбувається в умовах невизначеності, яка пов'язана не тільки з об'єктивними зовнішніми факторами, що впливають на господарську діяльність, але і з факторами, що виникають безпосередньо в системі бухгалтерського обліку. Такі фактори та їх наслідки можуть мати значний вплив на показники бухгалтерської (фінансової, внутрішньогосподарської) звітності і, отже, на прийняті управлінські рішення стосовно заходів по забезпеченню економічної безпеки підприємства та його стійкого функціонування [10, с. 145].

Проблематика бухгалтерських ризиків в даний час є недостатньо опрацьованим напрямком як бухгалтерського обліку, так і науки про ризики. З позицій забезпечення економічної безпеки, Л.В. Гнилицька [10, с. 145] під бухгалтерськими (інформаційними) ризиками розуміє ризики, пов'язані із спотворенням інформації, що виникають у системі бухгалтерського обліку і є наслідком певних подій. До них відносяться ризики, пов’язані з навмисним викривленням облікової інформації, порушенням режиму збереження бухгалтерської інформації, що становить комерційну таємницю, ризики, пов’язані з вибором способів і методів в обліковій політиці, відсутність належної кваліфікації бухгалтерського персоналу, а також неналежний рівень технічного забезпечення. Для цих ризиків найбільш притаманні ознаки невизначеності, оскільки можливість об'єктивно оцінити ймовірність їх настання в основному відсутня. Підприємницькі ризики (загрози), визнані в бухгалтерському обліку, – це ризики фінансово-господарського середовища, що характеризують наслідки подій, які чинять (чи здатні чинити) суттєвий вплив на діяльність підприємства. Очевидно, що інформація про наслідки впливу підприємницьких ризиків на фінансово-господарську діяльність суб’єкта господарювання має велике значення для прийняття обґрунтованих управлінських рішень внутрішніми і зовнішніми користувачами не тільки щодо поточного становища підприємства, а й з урахуванням стратегії його діяльності.

Поповенко Н.С. позиціонує інформаційні ризики як небезпеку виникнення збитків внаслідок застосування компанією інформаційних технологій. Інакше кажучи, інформаційні ризики пов’язані із створенням, передачею, збереженням та використанням інформації за допомогою електронних носіїв чи інших засобів зв’язку. У зв’язку з цим їх можна поділити на дві категорії: 1) ризики, які викликані витоком інформації й використанням її конкурентами чи співробітниками з метою, що може нашкодити бізнесу; 2) ризики технічних збоїв роботи каналів передачі інформації, що може призвести до збитків [33, с. 179]. Робота щодо мінімізації таких ризиків полягає у попередженні несанкціонованого доступу до даних, а також аварій та збоїв обладнання. Процес мінімізації інформаційних ризиків слід розглядати комплексно: спочатку виявляються можливі проблеми, а потім визначається, якими чином їх можна вирішити.

Крім того, на сьогодні у вітчизняній системі бухгалтерського обліку відсутні законодавчо закріплені організаційно-методичні розробки й рекомендації щодо відображення всіх фактів господарського життя, які мають різний рівень ймовірності виникнення й впливу на господарську діяльність підприємства в умовах невизначеності та ризику підприємницької діяльності. У зв’язку з цим, частими є випадки, на які наголошує В.З. Семанюк: “Показники рентабельності, ліквідності, платоспроможності та подібні їм, побудовані на основі даних фінансового обліку, дають нам інформацію про фінансовий стан в ретроспективі, а на основі якої інформації керівнику прийняти стратегічне рішення? Потрібні показники, які заздалегідь сигналізуватимуть про негативні тенденції, дозволять виявляти причини дестабілізації для прийняття відповідних корегуючих впливів, дадуть відповідь на питання “Що робити?” [40, с. 304].

Висока якість системи обліку у всіх суттєвих аспектах знижує до прийнятного рівень інформаційного ризику для її користувачів. Недаремно поняття якості в обліку тісно переплетене з поняттям інформації, як продукту облікової системи та, в основному, визначається її якісними характеристиками. Під якістю облікової системи слід розуміти її здатність продукувати (створювати) інформацію про внутрішнє і зовнішнє середовище підприємства, що відрізняє його від інших економічних наук та дозволяє ідентифікувати певні процедури й методики на належність до облікової системи [41].

Хоча є дослідники, зокрема Н.В. Наконечна [30], які вважають, що інформаційні системи обліку мають низку уразливих місць. Є дві категорії загроз: активні (комп’ютерне шахрайство та комп’ютерний саботаж) та пасивні (помилки системи). Незахищеність інформаційних систем обліку призводить до надмірних витрат, недостатніх доходів, втрати активів, недостовірного обліку, перешкод у бізнесі, санкцій, збитків з вини конкурентів, шахрайства та присвоєння.

Ризик, пов’язаний з безпекою, – це очікуваний розмір втрат за визначений період з огляду на надійність засобів захисту. Слабкі місця виникають внаслідок того, що немає ніякого засобу для запобігання акту порушення безпеки або є імовірність, що засіб забезпечення безпеки на визначеній ділянці автоматизованої системи не спрацює проти специфічного інциденту, що відбудеться.

Управління загрозами здійснюється через запровадження заходів безпеки та планів на випадок непередбачених подій. Заходи безпеки передбачають попередження та розпізнання загроз. Для захисту інформації в автоматизованих облікових системах створюють комп’ютерну систему безпеки. Комп’ютерні системи безпеки розробляють на основі застосування визначених методів аналізу систем, розроблення, впровадження, функціонування оцінки та контролю.

Для ефективного управління процесами визнання й нівелювання ризиків, які пов’язані з безпекою підприємства, слід дотримуватися наступної послідовності: 1) ідентифікація засобів захисту на визначеній ділянці ведення бухгалтерського обліку; 2) оцінка надійності засобів захисту на цій ділянці; 3) оцінка ймовірності, що акт порушення безпеки буде успішний з огляду на набір засобів захисту на цій ділянці та їх надійність; 4) оцінка втрат, що понесе підприємство, якщо акт порушення безпеки обійде засоби захисту в цьому місці системи.

За таких умов для побудови комплексної системи інформаційної безпеки підприємства, адекватної сучасним умовам господарювання, необхідним виступає ранжування та обґрунтування кожного виду загроз інформаційній безпеці підприємства, яку несуть в собі інформаційні потоки системи бухгалтерського обліку, що обслуговують усі бізнес-процеси сучасного суб’єкта господарювання в умовах ризику та невизначеності, що і слугує перспективою подальших досліджень. Отже, побудова надійної системи захисту дуже складний процес, який охоплює безліч різних етапів: оцінка інформації, яка має бути захищена, аналіз ризиків, вибір контрзаходів, оцінка ефективності системи захисту і супроводження. І тільки за системного підходу у вирішенні питання забезпечення інформаційної безпеки і економічної безпеки підприємства загалом, а також комплексного використання різних засобів захисту на всіх етапах життєвого циклу системи, починаючи зі стадії проектування, можна досягти результатів. А саме, певних фінансових результатів своєї діяльності і фінансової стійкості, технологічної незалежності і високої конкуренції технологічного потенціалу; високої ефективності організаційної структури; якісного правового захисту всіх аспектів діяльності; захисту інформаційного середовища; безпеки персоналу, власності і комерційних інтересів.

Висновки та перспективи подальших досліджень.

1. В інформаційному суспільстві інформація відіграє роль домінантного чинника розвитку економічних систем та отримує статус економічного ресурсу, адже під впливом інформації трансформуються форми економічної діяльності, приймаються управлінські рішення та розробляються стратегії розвитку підприємств на довгостроковий період. Не зважаючи на зростання важливості інформації, її наявності, рівня розвитку та ефективності використання засобів її обробки та передачі, економічна література з проблем теорії обліку, його функціонування та організації не приділяє уваги інформаційним ресурсам, або ж лише констатує факт їх існування, а склад інформаційних ризиків, які несе в собі бухгалтерська інформація, є малодосліджуваними.

2. Бухгалтерська інформація виступає внутрішнім ресурсом забезпечення інформаційної безпеки, яка в собі несе суттєві ризики діяльності підприємства. Комплексний аналіз сукупності внутрішніх та зовнішніх загроз, які впливають на дотримання економічної безпеки підприємства, знижує ризик виникнення викривлень в обліку через несприятливі зовнішні впливи на автоматизовану облікову систему підприємства, а також формування множини показників, за значенням яких можна виявляти, контролювати та нівелювати негативні тенденції у прийнятті виважених управлінських рішень.

Викладені в статті пропозиції є основою для подальшого формування організаційного механізму інформаційної безпеки підприємницької діяльності та розвитку її методичного забезпечення в частині бухгалтерської інформації.

Список використаних літературних джерел:

1. *Аврова И.А.* Управленческий учет / И. А. Аврова. – М. : Бератор-Пресс, 2003. – 175 с. 2. АСУ и проблемы теории бухгалтерского учета [Text] / В.Ф. Палий ; соавт. Соколов Я.В. – М. : Финансы и статистика, 1981. – 224с. 3. *Бармен С.* Разработка правил информационной безопасности: Пер. с англ. − М.: Издательский дом “Вильямс”, 2002. − 208 с. 4. *Білокомірова Я.М.* Інформаційне забезпечення економічної безпеки підприємницької діяльності / Я.М. Білокомірова // Вісник економіки транспорту і промисловості. – 2010. – № 29. – С. 308-312. 5. *Бондар М.* Облікова-аналітична інформація в управлінні підприємницькою діяльністю [Текст] / М. Бондар // Економічний аналіз: збірник наукових праць кафедри економічного аналізу ТНЕУ. – 2010. – № 6. – С.13-16. 6. *Буров И.В.* Свобода обращения социальной информации как показатель динамики развития общества / И.В.Буров // Философская и социалистическая мысль. – 1989. – № 2. – С. 84–87. 7. Бухгалтерский учет: учеб. для студ. вузов / [П.С. Безруких, В.Б. Ивашкевич, Н.П. Кондраков, В.Ф. Палий, В.Д. Новодворский] ; под ред. П.С. Безруких. – М.: Бухгалтерский учет, 1994. – 527 с. 8. *Волеводэ А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводэ. –М.: ООО Издательство ”Юрлитинформ“, 2002. –496 с. 9. *Галатенко В.А.* Основы информационной безопасности. − М.: Изд-во "Интернет-университет информационных технологий − ИНТУИТ.ру", 2003. − 280 с.: ил. 10. *Гнилицька Л.В.* Напрями удосконалення облікової системи з метою забезпечення економічної безпеки суб’єктів господарювання / Л.В. Гнилицька // Комунальне господарство міст. – 2011. – № 10. – С. 144-153 11. *Гнилицька Л.В.* Проблеми та шляхи вдосконалення обліково-аналітичного забезпечення економічної безпеки підприємства / Л.В. Гнилицька // Бухгалтерський облік і аудит. – 2011. – № 10. – С. 23. 12. *Добровський В.М.* Управлінський облік: [навч.-метод. посіб.] / В.М. Добровський, Л.В. Гнилицька, Р.С. Коршикова. – Київ : КНЕУ, 2003. – 191 с. 13. *Доля А.* Сколько стоит утечка информации на самом деле? [Электронный ресурс] / А. Доля // CNEWS. – Режим доступа : http://safe.cnews.ru/. 14. *Донець Л.І.* Економічна безпека підприємства: [навч. пос.] / Л.І. Донець, Н.В. Ващенко. – К.: Центр учбової літератури, 2008. – 240 с. 15. *Живко М.О.* Основні чинники інформаційної безпеки підприємства / М.О. Живко, Х.З. Босак // Актуальні проблеми економіки. – 2009. – № 8(98). – С. 67-74. 16. Закон України "Про інформацію" від 02.10.1992 № 2657-XII / [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2657-12 17. Закон України "Про підприємництво" від 07.02.1991 № 698-XII / [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/698-12 18. *Ілляшенко С.М.* Економічний ризик [Текст]: [навч. посіб. 2-ге вид., доп., перероб.] / С.М. Ілляшенко – К.: Центр навчальної літератури, 2004. – 220 с. 19. Інформаційні системи бухгалтерського обліку: [підручник] / [Ф.Ф. Бутинець, С.В. Івахненков, Т.В. Давидюк, Т.В. Шахрайчук]. – [2-тє вид., перероб. і доп.]. – Житомир : ПП “Рута”, 2002. – 544 с. 20. Как утекает информация? [Электронный ресурс]. – Режим доступа : http://www.securelist.com/ru/analysis/. 21. *Кириченко Є.* Теоретичні основи управлінського обліку / Є. Кириченко // Аудитор України. – 2006. – № 15. – С. 16-23. 22. *Клєбанова Т.С.* Моделі оцінки, аналізу та прогнозування економічної безпеки підприємства: [Текст] / Т.С. Клєбанова, Є.А. Сергієнко // Бізнес Інформ. – 2006. – № 8. – С. 65-72. 23. *Князєв С.О.* Іноземний досвід захисту важливих інформаційних ресурсів / С.О. Князєв // Бизнес и безопасность. – 2009. – № 3 (71). – С. 27-29. 24. *Ковалев Д.* Экономическая безопасность предприятия [Текст] / Д. Ковалев, Т. Сухорукова // Экономика Украины. – 1998. – № 10. – С. 48-51. 25. *Козаченко А.В.* Экономическая безопасность предприятия: сущность и механизм обеспечения: [монография] [Текст] / А.В. Козаченко, В.П. Пономарев, А.Н. Ляшенко. – К.: Либра, 2003. – 280 с. 26. *Кравчук О.Я.* Діагностика рівня та критерії оцінки корпоративної безпеки суб’єктів господарювання [Текст] / О.Я. Кравчук, П.Я. Кравчук // Економічні науки. Серія “Економіка та менеджмент”: Збірник наукових праць. Луцький державний технічний університет. – Випуск 1. Редкол.: відп. ред. д.е.н., проф. Герасимчук З.В. – Луцьк, 2004. – С. 85-109. 27. *Крилова О.* Всі секрети по кишенях / [Електронний ресурс]. – Режим доступу: www.rdwmedia.ru. 28. *Куркін Н.В.* Управління економічною безпекою розвитку підприємства: [монографія]. – Д.: АРТ-ПРЕСС, 2004. – 452 с. 29. *Мишин Ю.А.* Управленческий учет: управление затратами и результатами производственной деятельности: [монографія] / Ю.А. Мишин. – М. : Издательство “Дело и Сервис”, 2002. – 176 с. 30. *Наконечна Н.В.* Безпека автоматизованих облікових систем у системі економічної безпеки підприємства / Н.В. Наконечна // Вісник Львівської комерційної академії. – Сер.: Економічна. – Львів: Вид-во Львівської КА. – 2009. – Вип. 32. – С. 100-104. 31. *Пенькова І.В.* Інформаційні потоки в управлінні економічною безпекою держави / І.В. Пенькова, О.І. Левченко // Сучасні перспективи розвитку систем економічної безпеки держави та суб’єктів господарювання: [монографія] / За ред. проф. Мігус І.П. – Черкаси: ТОВ “МАКЛАУТ”. – Черкаси, 2012. – 636 с. – С. 573. 32. *Попов С.В.* Проблеми інформаційної безпеки України / С.В. Попов, О.О. Бойченко // Форму права. – 2011. – № 1. – С. 798-801. 33. *Поповенко Н.С.* Інформаційна безпека на підприємствах малого бізнесу / Н.С. Поповенко, Г.О. Полуніна // Экономика Крыма. – 2012. – №3(40). – С. 177-181. 34. Про проблеми захисту прав інтелектуальної власності та шляхи їх вирішення / Рішення Колегії МОН України від 4 грудня 2003 р. / [Електронний ресурс]. – Режим доступу: http://lawua.info/jurdata/dir212/dk212537. htm. 35. *Прокоф'єва Д.М.* Підприємницьке шпигунство в системі інформаційних злочинів // Украинский центр информационной безопасности / www.bezpeka.com/library/lib_aspect.html. 36. *Пушкар М.С.* Ідеальна система обліку: концепція, архітектура, інформація: [Текст] / М.С. Пушкар,

М.Г. Чумаченко – Тернопіль: Карт-бланш, 2011. – 336 с. 37. *Пушкар М.С.* Створення інтелектуальної системи обліку: [Текст] [монографія] / М.С. Пушкар. – Тернопіль: Карт-бланш, 2007. – 152 с. 38. *Реверчук Н.Й.* Управління економічною безпекою підприємницьких структур [Текст]: монографія / Н.Й. Реверчук. – Львів: ЛБІ НБУ, 2004. – 195 с. 39. *Савва О.П.* Роль інформації в досягненні конкурентоспроможності / О.П. Савва // Вісник КНУТД. – 2007. – № 3. – С. 103-111. 40. *Семанюк В.З.* Інформаційні ресурси як інструмент підвищення ефективності бізнесу / В.З. Семанюк // Інноваційна економіка. – 2012. – № 10(36). – С. 304-307 41. *Семанюк В.З.* Критерії якості облікової системи підприємства: теоретичний аспект [Текст] / В.З. Семанюк // Вісник ДонНУЕТ; Серія Економічні науки. – 2011.– № 3/2 (51). – С. 232-237. 42. *Симкин Л.С.* Программы для ЭВМ: правовая охрана (правовые средства против компьютерного пиратства) / Л.С. Симкин. – М.: Издательство "Городец",1998. – 208 с. 43. *Сопко В.В.* Бухгалтерський облік в управлінні підприємством: [навч. посіб.] / В.В. Сопко. – К.: КНЕУ, 2006. – 526 с. 44. *Степанова О.М.* Інформаційна безпека в умовах розвитку інформаційної системи підприємства / О.М. Степанова, Л.М. Дегтярьова // Інформаційна безпека. – 2009. – № 1(1). – С. 59-63. 45. *Стоун Т.* Управленческий учет / Т. Стоун; [пер. с. англ. под ред. Н.Д. Эриашвили]. – М. : Аудит, ЮНИТИ, 1997. – 179 с. 46. *Ткачук Т.* Формування системи інформаційної безпеки бізнесу / Т. Ткачук // Бізнес и безопасность. – 2007. – № 4. – С. 19-23. 47. Управленческий учет как составляющая часть единой учетной системы предприятия; под. ред. Т.К. Киселева. – Запорожье: Запорожский гос. центр научно-технической и экономической информации, 2004. – 68 с. 48. Управлінський облік в системі гірничорудних підприємств [Текст]: дис... д-ра екон. наук: 08.06.04 / Нападовська Любов Василівна; Київський національний економічний ун-т. – К., 2002. – 437 с. 49. Утечка из PricewaterhouseCoopers: украдены данные 77 тыс. госслужащих // Информационная безопасность. – 2010. – № 3. – С. 77-86. 50. Утечка информации в 2010 году. WikiLeaks // Информационная безопасность. – 2010. – № 4. – С. 12-26. 51. Экономическая и национальная безопасность [Текст] / Под ред. Е.А. Олейникова. – М.: Издательствово "Экзамен", 2004. – 768 с. 52. *Юзва Р.П.* Оцінка якості інформаційного забезпечення управління підприємством / Р.П. Юзва // Інноваційна економіка. – 2011. – № 2(21). – С. 44-47 53. *British Standard*. Code of practice for information security management British Standards Institution, BS 7799:1995 54. *British Standard*. Information security management systems − Specification with guidance for use, British Standards Institution, BS 7799-2:2002 55. *Kavun S*. Statistical analysis in area of economic and information security. ES INFECO: International research portal of information and economic security, 2011-2012 / [Electronic resource]. – Access mode: http://www.infeco.net

БОРИМСЬКА Катерина Павлівна – кандидат економічних наук, доцент, докторант кафедри бухгалтерського обліку Житомирського державного технологічного університету.

Наукові інтереси:

– облікове забезпечення фінансово-економічної безпеки підприємств України;

– проблемі аспекти фінансово-економічної безпеки діяльності підприємств Республіки Польща;

– теорія й методологія розвитку вчення про рахунки бухгалтерського обліку;

– історія бухгалтерського обліку.

Стаття надійшла до редакції 01.02.2013 р.