використання нововведень, але і його приріст порівняно з аналогами. Порівняльна оцінка ефективності нововведення сприяє вибору найоптимальнішого варіанта з числа можливих і визначення його впливу на економічні показники господарської діяльності підприємства.

2. При оцінюванні ефективності проекту необхідно провести розподіл, як трансформуються нововведення, адже на початку створення ідея завжди є чимось новим, а на виході перетворюється або в інновацію, або в удосконалений продукт. Такий розподіл пов'язаний з тим, що характеристики вдосконаленого продукту здебільшого вже відомі, а натомість інновації окреслені нечіткими даними.

3. Методи оцінки ефективності інновацій ґрунтуються на системі оціночних показників, ураховуючи інтереси держави, виробників, споживачів, інвесторів, відображаючи необхідні для кожного з них показники з урахуванням ролі всіх елементів у процесі інноваційної діяльності.

4. Також методи оцінки ефективності повинні містити показники, що відображають інтегральний (загальний) ефект від створення, виробництва й експлуатації нововведень. Такий підхід дозволяє здійснити узагальнюючу (комплексну) оцінку ефективності нововведення і розподілити здобутки кожного елемента під час упровадження інновацій.

Динамічний розвиток сучасної економіки, швидкість науково-технічного прогресу, зростаюча конкуренція зумовлюють покращення вибору пріоритетного проекту на основі комплексного зіставлення фінансових, часових та людських ресурсів, планових витрат з очікуваним результатом.

Література

1. Досліджуючи стратегічні ризики [Електронний ресурс]. –

2. Режим доступу: http://www2.deloitte.com/ua/uk/pages/governance-risk-and compliance/articles/exploring-strategic-risk.html

3. G. Kendall, S. Rollins, «Advanced Project Portfolio Management and the PMO: Multiplying ROI at Warp Speed», J. Ross Publishing, 2003, pp. 69–79.

УДК 657

Шевчук О. А.,
Тернопільський національний економічний університет

АНАЛІЗ ЗАГРОЗ У КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ БУХГАЛТЕРСЬКОГО ОБЛІКУ (КІСБО)

Проблеми організації обліку на підприємствах змушують бухгалтерів постійно оптимізувати процес обробки інформації, вдосконалювати форми обліку, змінювати ручний спосіб обробки інформації на комп'ютерний. Тому

виникає нагальна необхідність збереження та обмеження доступів до вхідної інформації.

Проблемні аспекти комп'ютерних систем бухгалтерського обліку досліджуються фахівцями різних галузей знань. Зокрема, ці проблеми досліджували Завгородній В. П., Івахненков С. В., Муравський В. В., Ситник В. Ф., Шквір В. Д. Дослідження вищеперерахованих проблем ускладнюється тією обставиною, що потребує компетентності дослідника як у бухгалтерському обліку, так і в сучасних інформаційних системах та технологіях.

Комп'ютерна інформаційна система бухгалтерського обліку (КІСБО) – це сукупність елементів, які взаємодіють між собою в процесі обробки облікової інформації підприємства. До елементів КІСБО належать інформація, програмні, технічні, організаційні, алгоритмічні, документальні та інші засоби, функціональні компоненти тощо [1, с.58].

Комп'ютерні інформаційні системи мають уразливі місця, тобто слабкі сторони системи. Загроза КІСБО – це потенційне використання уразливого місця. Є дві категорії загроз: активні і пасивні. Активні загрози включають комп'ютерне шахрайство та комп'ютерний саботаж. Пасивні загрози - це помилки системи (пошкодження окремих компонентів обладнання) та катастрофи. Доступність ризику (незахищеність) інформаційних систем бухгалтерського обліку призводить до надмірних витрат, недостатніх доходів, втрати активів, недостовірного обліку, перешкод у бізнесі (закриття бізнесу), санкцій, збитків з вини конкурентів, шахрайства та присвоєння.

Власник інформації самостійно забезпечує захист інформації від несанкціонованого доступу. Захист інформації - сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. Несанкціонований доступ - доступ до інформації, що здійснюється з порушенням встановлених в АС правил розмежування доступу [2]. Об'єктами захисту є інформація, що обробляється в АС, права власників цієї інформації та власників АС, права користувача. Захисту підлягає будь-яка інформація в АС, необхідність захисту якої визначається її власником або чинним законодавством. Захист інформації в АС забезпечується шляхом: дотримання суб'єктами правових відносин норм, вимог та правил організаційного і технічного характеру щодо захисту оброблюваної інформації; використання засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому, засобів захисту інформації, які відповідають встановленим вимогам щодо захисту інформації (мають відповідний сертифікат); перевірки відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому встановленим вимогам щодо захисту інформації; здійснення контролю щодо захисту інформації.

Система захисту інформації – це підсистема організації, яка контролює спеціальні ризики, пов'язані з комп'ютерними інформаційними системами. Для захисту інформації в КІСБО створюється комп'ютерна система безпеки. Комп'ютерна система безпеки має основні елементи будь-якої інформаційної системи, такі як апаратне забезпечення, бази даних, процедури та звіти [3, с.126].

Головним методом попередження активних загроз стосовно шахрайства та саботажу є імплементація послідовних рівнів заходів контролю за доступом до веб-сайту, до корпоративної системи та до файлів. Метою заходів контролю за доступом до сайту є встановлення фізичного бар'єру до комп'ютерних ресурсів для осіб, які не мають дозволу. Цей бар'єр слід застосовувати до апаратного забезпечення, областей введення даних, бібліотек даних, областей виведення даних та монтажу зв'язку. Слід вимагати, щоб усі користувачі носили захисні ідентифікаційні картки з фотографіями. Заходи контролю за доступом до системи – це заходи контролю за програмним забезпеченням, розроблені для того, щоб встановити перешкоди для використання системи несанкціонованими користувачами. Ці заходи контролю установлюють користувачів, які мають дозвіл доступу до системи шляхом використання ідентифікаційних даних, паролів, адрес IP та пристроїв до апаратного забезпечення.

Щодо організаційної структури КІСБО керівництвом застосовують такі дії: розподіл обов'язків; нагляд; вимушені відпустки та зміна роботи (посади); подвійний контроль; «судовий облік». Розподіл обов'язків передбачає: розподіл функцій дозволу та запису операцій, розподіл функцій дозволу та зберігання активів, розподіл функцій запису операцій та зберігання активів. Застосовують наступні контрольні процедури: перевірка виконання операцій відповідно до розподілених обов'язків; перевірка застосування затверджених бланків документів та записів; перевірка здійсненого доступу до активів відповідно до санкцій керівництва; незалежні перевірки стану активів у підзвітності матеріально відповідальних осіб та результатів їх діяльності; перевірка процесу обробки інформації у відповідності з дозволами, її точності та повноти.

Пасивні загрози включають такі проблеми як відключення електроенергії та збої в роботі комп'ютерів. Заходи контролю за такими загрозами можуть бути попереджуючими та коригуючими. Попереджуючі заходи контролю передбачають використання резервних компонентів інформаційних систем. Якщо одна частина системи не спрацьовує, резервна частина миттєво підключається і система продовжує функціонувати з невеликою паузою чи зовсім без затримки. Коригуючі заходи контролю передбачають використання резервних файлів для виправлення помилок [4, с.465].

Таким чином підсумуємо вище викладене і зазначимо, що нині власник інформації самостійно забезпечує захист інформації від несанкціонованого доступу. Захист інформації – сукупність організаційно-технічних заходів і

правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

Література

1. Деньга С. М. Інформаційні системи і технології обліку [Текст]: опорний конспект лекцій / С. М. Деньга. – Полтава: РВВ ПУСКУ, 2013. – 107 с.

2. Про захист інформації в автоматизованих системах: Закон України від 5.07.1994 р. № 81//94-ВР. // Галицькі контракти. – 1996. – №47 – с. 44-50.

3. Шевчук О. А. Імплементація автоматизованої інформаційної системи обліку в практичну діяльність вітчизняних підприємств [Текст] / О.А. Шевчук // Облік, аналіз, аудит і оподаткування в умовах глобалізації економіки. Тези доповідей І Міжнародної науково-практичної конференції, м. Ужгород, 21 квітня 2017 р. – Ужгород: УжНУ «Говерла», 2017. – С.126-127.

4. Shevchuk O. Automation of accounting in agro-industrial enterprises with the use of unmanned aerial vehicles (uavs) / O. Shevchuk, V.Muravskyi, N.Pochynok // Business Economics, Issue 4 (2), (October). Volume 52. Palgrave Macmillan Ltd., 2017. – P. 460-474.

УДК 657

Шестерняк М. М.,
Тернопільський національний економічний університет

ЕКОНОМІЧНИЙ АНАЛІЗ: ПЕРСПЕКТИВИ РОЗВИТКУ

Економічний аналіз є засобом створення основного ресурсу постіндустріальної економіки – інформації, невід'ємним елементом у діяльності підприємств, адже досліджує їх функціонування, вивчає резерви виробництва, дає оцінку стану аналізованого об'єкта, є базою для прийняття обґрунтованих управлінських рішень на основі наявної інформації, допомагає визначити напрямки підвищення ефективності діяльності та дозволяє спрогнозувати розвиток у майбутньому. На початку свого розвитку та становлення економічний аналіз був пов'язаний тільки з обліком та статистикою, однак з поглибленням економічної роботи на підприємстві виникає необхідність у виділенні аналізу як окремої системи знань, що вивчає господарські процеси, їх взаємозв'язок, взаємозалежність і взаємозумовленість. Тому перспективи розвитку економічного аналізу як практичного, так і теоретичного спрямування є актуальною проблемою сьогодення.

Теоретичну та методологічну базу економічного аналізу досліджували видатні вчені, зокрема: М. Д. Білик, Ф. Ф. Бутинець, В. А. Дерій, І. П. Житна, Л. М. Кіндрацька, І. Д. Лазаришина, Б. М. Литвин, Є. В. Мних, Ю. С. Цал-Цалко, М. Г. Чумаченко, С. І. Шкарабан та інші [1-6]. Динамічні зміни в