УДК 657

Шевчук О. А.,
к.е.н., доцент кафедри обліку і оподаткування,
Тернопільський національний економічний університет

ПРОБЛЕМНІ АСПЕКТИ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ СИСТЕМ БУХГАЛТЕРСЬКОГО ОБЛІКУ

Проблеми організації обліку на підприємствах змушують бухгалтерів оптимізовувати 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 в 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, 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.

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.

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 [3, с.103]. Таким чином, власник інформації самостійно забезпечує захист інформації від несанкціонованого доступу.

Література

1. Деньга С.М. Інформаційні системи і технології обліку. Опорний конспект лекцій. – Полтава: РВВ ПУСКУ, 2013. – 107 с.

2. Шевчук О.А. Автоматизація обліку: сьогодення та майбутнє / О.А. Шевчук // Сучасні детермінанти фіскальної політики: локальний та міжнародний вимір. Збірник матеріалів Третьої Міжнародної науково-практичної конференції. Тернопіль, 10 вересня 2019 р.– Тернопіль: ТНЕУ, 2019. – С.299-301.

3. Shevchuk O. Management accounting of the settlements with contractors in innovative environment of business communications / O. Shevchuk, V.Muravskyi, Z.-M.Zadorozhnyi, Yu.Sudyn // Маркетинг і менеджмент інновацій. – Суми: СумДУ, 2018. – № 2. – С.103-112.