трансформація - операція - трансферт, аутсорсинг допоміжних операцій, передача-переклад постійних витрат в змінні.

Але, безумовно, віддавати або не віддавати функції бухгалтерського обліку на аутсорсинг рекомендацій немає. Це питання кожне підприємство вирішує для себе, виходячи зі своїх цілей, власного розсуду шляхів їх досягнення і наявності ресурсів.

Література.

1. Райзберг Б. А. Современный экономический словарь / Б. А. Райзберг, Л. Ш. Лозивский, Е. Б. Стародубцева. – М. : ИНФРА-М, 2006. – 356 с.

2. Матвій І. Є. Аутсорсинг в діяльності промислових підприємств: основні переваги та загрози / І. Є. Матвій // Прометей: регіональний збірник наукових праць з економіки. – Донецьк : ДЕГІ, 2008. – № 1 (25). – С. 184-189.

3. Фомушкіна В. А. Сучасний стан, переваги та недоліки аутсорсингу бухгалтерського обліку / В.А. Фомушкіна // Управління розвитком. – 2013. – № 17 (157). – С. 33–35.

4. Кононова І. Аналіз попиту і оцінка якості послуг аутсорсинга в Україні : [Електронний ресурс]. – Режим доступу : http://job.ukr.net/articles/analiz-vostrebovannostii-ocenka-kachestva-uslug-autsorsinga-v-ukraine/

ПРОБЛЕМНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ БУХГАЛТЕРСЬКОГО ОБЛІКУ

Лобач К.Р., студент
Науковий керівник: Голеско І.О., ст. викладач
Харківський національний автомобільно-дорожній університет

Нагальні потреби суб’єктів господарювання та інших пересічних користувачів – споживачів фінансово-економічного контенту в обліковій інформації змушують бухгалтерів направляти зусилля на пошук та впровадження прогресивних програмних продуктів, які дозволяють постійно оптимізувати процес обробки інформації, удосконалювати форми обліку, все більше замінювати ручний спосіб обробки інформації на комп'ютерний. Інтелектуалізація автоматизованих робочих місць на базі новітньої комп'ютерної

техніки та інтелектуального інтерфейсу забезпечує діалогове спілкування бухгалтерів, фахівців інтелектуальної праці з інформаційною системою і використання її при виконанні функцій бухгалтерського обліку і контролю в господарському механізмі за умов ринкової економіки.

Разом з розвитком комп'ютеризації облікового напрямку праці набули актуальності питання вирішення супутніх проблем, притаманних процесам використання мережевих програмних продуктів, а саме: захист інформації від несанкціонованого втручання, юридична доказовість електронних первинних документів, можливість втрати чи псування інформації під час проникнення комп'ютерних вірусів, захист облікової інформації тощо.

Вказані проблеми комп'ютерних інформаційних систем бухгалтерського обліку потребують розгляду водночас фахівцями декількох галузей знань: фахівцями з інформаційних систем, бухгалтерами, менеджерами.

Структурно-організуючою підставою для вирішення питань експлуатації та захисту інформаційного середовища є Комп'ютерна інформаційна система бухгалтерського обліку (КІСБО), яка представляє собою 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.

Основу права власності на інформацію складають врегульовані законом суспільні відносини щодо володіння, користування і розпорядження нею, які виникають на підставі створення інформації своїми силами і за свій рахунок, договору на створення інформації, договору, в якому міститься інформація щодо переходу права власності на інформацію до іншої особи.

Комп'ютерні інформаційні системи мають вразливі місця, тобто слабкі сторони системи. Загроза КІСБО – це потенційне використання вразливого 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) і катастрофи. Доступність (незахищеність) інформаційних систем бухгалтерського обліку призводить до надлишкових витрат, зниження доходів, втрат

активів, недостовірності обліку, перешкод в бізнесі (закриття бізнесу), санкцій, збитків з вини конкурентів, шахрайства та привласнення [1].

Зазвичай загрозу для комп'ютерної інформаційної системи можуть становити три групи осіб, а саме: 1) персонал, який обслуговує інформаційні системи; 2) користувачі; 3) зловмисники [2].

Персонал, який обслуговує інформаційні системи, – це фахівці з експлуатації та ремонту комп'ютерного та мережевого обладнання, програмісти, оператори мережі, адміністративний персонал інформаційних систем, фахівці з контролю за даними. Користувачі складаються з груп працівників, функціональна сфера яких належить до сфери обробки даних. У КІСБО – це бухгалтери, матеріально відповідальні особи і менеджери. Зловмисники – це будь-які сторонні особи, які приєднуються до обладнання, електронних даних і файлів без належного дозволу. Дослідження вказують, що навмисні дії складають до 45 % причин виникнення кризового стану інформаційних систем [1].

Таким чином, проблемність протидії загрозам інформаційним комп’ютерним системам бухгалтерського обліку полягає в організації захисту, як сукупності організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи комп’ютерних інформаційних систем (КІС) та осіб, які користуються інформацією.

Захисту підлягає будь-яка інформація в КІС, необхідність захисту якої визначається її власником або чинним законодавством.

Захист інформації в КІС забезпечується шляхом: виконання суб'єктами правових відносин норм, вимог і правил організаційного і технічного характеру щодо захисту оброблюваної інформації; використання, організації контролю та регламентної перевірки комп’ютерного та мережевого обладнання, програмного забезпечення, засобів зв'язку, засобів захисту інформації, які відповідають встановленим вимогам щодо її захисту (мають відповідний сертифікат).

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

Існує два основні підходи до аналізу вразливих місць і загроз системи: кількісний підхід і якісний підхід до оцінки ризику. При кількісному підході до оцінки ризику кожен рівень доступності ризику потенційних збитків обчислюється, як результат вартості окремого збитку, помноженого на достовірність його виникнення. При застосуванні кількісного підходу може бути складно оцінити кожен випадок збитку і достовірність його виникнення, а також передбачити майбутні події. Якісний підхід до оцінки ризику показує вразливі місця і загрози системи, суб'єктивно розставляючи їх в порядку важливості для сукупної доступності ризику потенційних збитків. Незалежно від застосовуваного методу будь-який аналіз повинен включати оцінку доступності ризику потенційних збитків, принаймні таких як: припинення виробництва, втрата програмного забезпечення, втрата даних, втрата апаратного забезпечення, втрата виробничих потужностей, втрата послуг і працівників [3].

Управління погрозами здійснюється через впровадження заходів безпеки і планів на випадок непередбачених подій. Розрізняють загальні заходи контролю і заходи контролю прикладних програм. Заходи контролю інформаційних систем покликані забезпечити впровадження елементів внутрішнього контролю всередині кожного з операційних циклів організації. Можна виділити чотири основних цикли операцій: доходів, витрат, виробництва і фінансовий.

Основним способом попередження активних загроз щодо шахрайства і саботажу є впровадження послідовних рівнів заходів контролю за доступом до КІС, сайту і файлам, тобто встановлення фізичного бар'єру до комп'ютерних ресурсів для осіб, які не мають дозволу. Цей бар'єр слід застосовувати до апаратного забезпечення, областям введення даних, бібліотек даних, областей виведення даних і операцій зв'язку. Заходи контролю за доступом до КІС – це заходи контролю за програмним забезпеченням, розроблені для того, щоб встановити перешкоди для використання системи несанкціонованими користувачами. Їх встановлюють користувачі, які мають дозвіл доступу до системи, шляхом використання ідентифікаційних даних, паролів, адрес IP і пристроїв апаратного забезпечення.

Таким чином, інформація, як суспільний продукт, потребує належного захисту, оскільки інформаційні ресурси є первинним факторіальним підґрунтям економічного зростання країни.

Наразі на ринку інформаційних послуг представлені новітні розробки із запровадження практичних заходів захисту інформації в

КІСБО. Але, незважаючи на досягнуті позитивні результати проблемність захисту інформації в комп'ютерних інформаційних системах бухгалтерського обліку не може бути визнана вирішеною. Шляхи поліпшення ситуації в цій галузі застосування інформаційних систем полягають в забезпеченні надійного функціонального розмежування доступу до файлових підсистем організаційної структури КІС. При цьому належним чином повинна бути організована система регламентних перевірок та внутрішнього контролю КІС з додержанням вимог та рекомендацій щодо розмежування доступу до програмних продуктів різного галузевого застосування на підставі належного контролю інформації та обробки електронних документів.

Література.

1. Деньга С. М. Контроль організаційної структури комп'ютерної інформаційної системи бухгалтерського обліку (КІСБО) [Електронний ресурс] / Деньга С. М. – Режим доступу до сайту : http://nadoest.com/kontrole-organizacijnoyi-strukturi-kompyuternoyi-informacijnoy

2. Рудов О. П. Інформаційний захист системи 1С Підприємство / Рудов О. П., Романченко Т. П., Скріпкіна А. С. // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15 (204) ч.1. – С. 187-191.

3. Наконечна Н.В. Безпека автоматизованих облікових систем у системі економічної безпеки підприємства / Наконечна Н.В. // Вісник Львівської комерційної академії. – 2009. – Віп. 32. – С.

ФОРМА ФІНАНСОВИХ ІНВЕСТИЦІЙ «ІРО», ЯК ІНСТРУМЕНТ ЗАЛУЧЕННЯ КАПІТАЛУ

Рогова А., студентка
Науковий керівник: Голеско І.О., ст. викладач
Харківський національний автомобільно-дорожній університет

Необхідність підвищення успішності розвитку свого бізнесу вимагає від підприємств постійного пошуку інвесторів для залучення додаткових капіталовкладень, оскільки брак власних коштів є основною передумовою до необхідності виходити на фондові біржі. Наразі, вітчизняний ринок не здатний задовольнити потреби