УДК: 657

С.О. Логвіненко, магістрант, V курс, гр. ОАМ-22, ФОФ
Науковий керівник – к.е.н., доц. М.О. Козлова
Житомирський державний технологічний університет

ВНУТРІШНІЙ КОНТРОЛЬ НАЯВНОСТІ ТА ВИКОРИСТАННЯ КОМП'ЮТЕРНОЇ ТЕХНІКИ ЯК ВАЖЛИВА СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Інформаційна безпека підприємства містить у собі програмний захист інформації та захищеність апаратних засобів. Щодо програмного забезпечення, то аспекти його контролю та наявності на сьогодні досить широко досліджуються, здебільшого науковцями не облікового спрямування, тому зосередимо увагу на посиленні інформаційної безпеки за рахунок підвищеного контролю наявності та використання апаратної частини комп'ютерної техніки. Основними нашими завданнями є визначення суб'єктів і об'єктів контролю наявності та використання комп'ютерної техніки, періодичності його здійснення, специфіки та мети заходів, коригувальних дій та рішень за результатами контролю.

Хотілося б акцентувати увагу, що при використанні комп'ютерної техніки, питанню безпеки слід приділяти увагу не лише в програмній, а й в апаратній частині. Передусім слід застосовувати найпростіші превентивні заходи, наприклад, використання додаткових модулів комп'ютера (безперебійного блоку живлення, мережевого маршрутизатора тощо). Варто звернути увагу на його розташування. Пропонуємо розташовувати комп'ютерну техніку таким чином, щоб мінімізувати доступ до неї сторонніх осіб, а у випадках, коли це неможливо (комп'ютер для роботи з клієнтами) – облаштувати робочі місця мінімум двох працівників таким чином, щоб вони здійснювали контроль за діями один одного та попереджали доступ сторонніх осіб до комп'ютеризованого робочого місця. Наступним етапом є закріплення за комп'ютерами відповідальних осіб (передусім – МВО, а також чітко визначити і закріпити відповідальність основного користувача комп'ютера). Це, в першу чергу, дозволить закріпити за працівником відповідальність за працездатність свого комп'ютера, а також забезпечить більш пильний нагляд з його боку, чим, відповідно, зменшить ризик несанкціонованого втручання. Наочно послідовність здійснення контролю комп'ютерної техніки відображено на рисунку 1.

Метою здійснення контрольних заходів є забезпечення інформаційної безпеки підприємства, а також достовірності інформації у системі бухгалтерського обліку. Важливим методом внутрішнього контролю комп'ютерної техніки є її інвентаризація, а враховуючи специфічність облікових об'єктів, очевидним є те, що контроль наявності та використання засобів комп'ютерної техніки потребує здійснення специфічних заходів. Обов'язково слід проводити глибинну перевірку наявності складових комп'ютерної техніки, тобто якщо інвентарний номер на підприємстві присвоєний системному блоку, то в описі обов'язково має бути зазначено, які частини входять до цього системного блоку із зазначенням марок та моделей вузлів, а також їх характеристик.

Це дозволить впевнитись у первинній комплектації комп'ютера і у фізичному невтручанні у його роботу. Дану процедуру в наш час можна здійснювати двома шляхами: програмним та апаратним. Програмний полягає у знаходженні інформації про вузли системного блоку за допомогою їх опису у засобах керування операційної системи, а апаратний заключається у фізичному моніторингу складових комп'ютера, коли знімається кришка корпуса і здійснюється безпосередній огляд та фіксація розміщених у системному блоці частин. Для того щоб уберегти себе від витоку інформації і не допустити махінацій з боку працівників, перевірку краще всього здійснювати без присутності працівників, оскільки тоді вони не знатимуть напевне спосіб, що був застосований перевіряючим, а отже і не будуть впевнені, яким чином фальсифікувати інформацію: програмним чи апаратним.

Залежно від розміру підприємства, чисельності працюючих, рівня автоматизації та інших факторів визначається періодичність проведення інвентаризації, але обов'язковими випадками, як видно з рисунка 1, є придбання, ремонт чи модернізація, списання комп'ютерної техніки та випадки, передбачені законодавством (а саме: зміна МВО, складання річної звітності, ліквідація підприємства тощо), через що вони і не знайшли свого відображення на рисунку 1. Значно поліпшить результати в плані достовірності інформації раптовий характер інвентаризації. Бажано здійснювати контроль в оперативному режимі, але періодичну перевірку, яка повинна мати більш повний та глибинний характер, слід здійснювати хоча б раз в квартал із коригуванням на розміри фірми та інші, зазначені вище, фактори. Для середніх підприємств, зокрема, така періодичність є прийнятною.

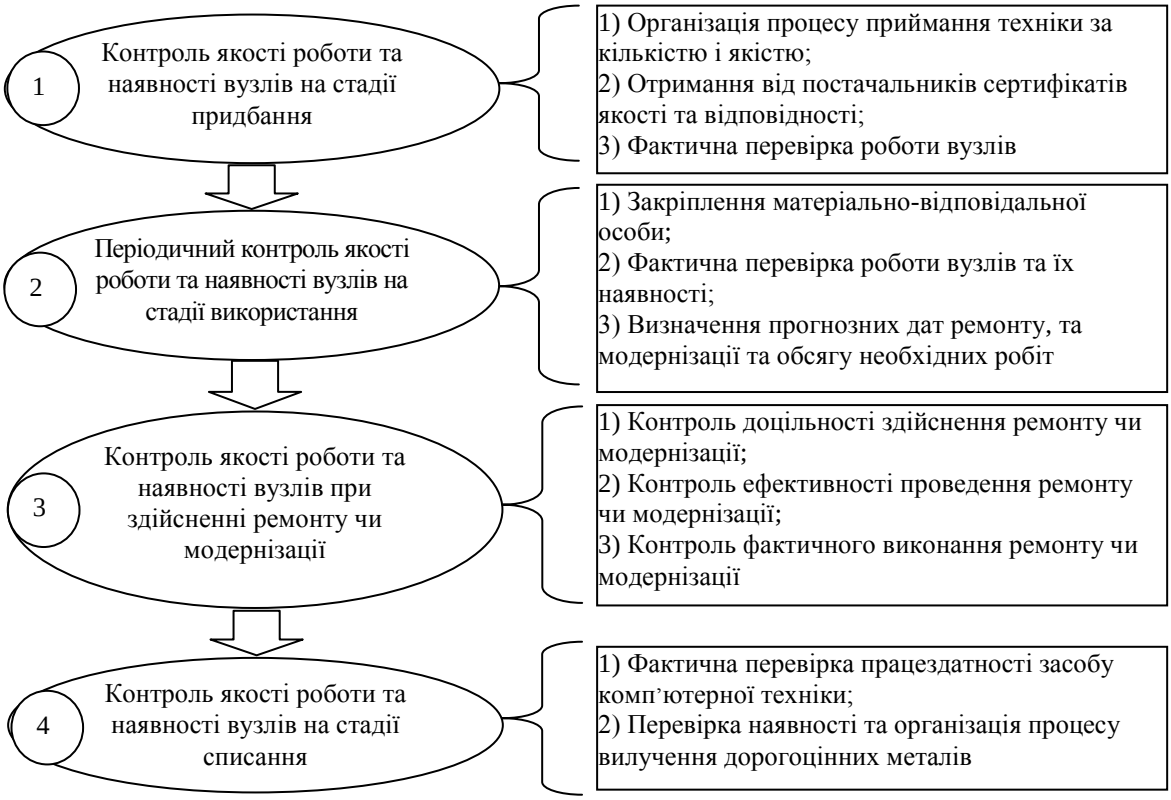

Рис. 1. Хронологічна послідовність здійснення контролю комп'ютерної техніки на підприємстві

Виходячи з викладеного вище, визначимо суб'єктів внутрішнього контролю. Ними, в першу чергу, повинні бути керівник (власник) та головний бухгалтер чи уповноважені особи, а також особа, в чиє безпосереднє користування передається комп'ютер. На окремих підприємствах для цього є спеціальні посади із різними назвами (ІТ-фахівець, програміст, системний адміністратор тощо) і спорідненими обов'язками, одним із яких є контроль за наявністю та використанням комп'ютерної техніки. Також матеріально-відповідальна особа, у відповідальність якої потрапляє комп'ютерна техніка, обов'язково має ознайомитися із її станом та якістю роботи. У випадках, якщо на підприємстві немає працівника, компетентного з даного питання, цю роль має виконувати бухгалтер, оскільки він несе відповідальність за достовірність та повноту відображення у системі бухгалтерського обліку інформації про стан справ на підприємстві. Стосовно об'єктів контролю, то ними є наявність та використання апаратних засобів та вузлів, працездатність та якість їх роботи.

Контроль використання містить: контроль використання за прямим призначенням; контроль за дотриманням користувачем правил техніки безпеки; контроль за дотриманням правил інформаційної безпеки користувачем під час роботи; контроль ефективності (обсяг витраченого часу на виконання завдань порівнюється із загальним часом роботи комп'ютера) та раціональності використання (потужний комп'ютер має використовуватися для складних обчислень та зберігання значних обсягів інформації). Суб'єкти контролю мають постійно інформувати вище керівництво щодо ефективності та раціональності використання наявного апаратного забезпечення, надавати пропозиції та рекомендації щодо впровадження ресурсозберігаючих заходів, необхідності та доцільності здійснення поточного та капітального ремонту і модернізації, що дозволить оптимізувати роботу апаратного забезпечення та знизить ймовірність ризику виникнення загроз інформаційній безпеці підприємства. З огляду на викладене вище варто наголосити, що слід приділяти достатньо уваги безпеці комп'ютерної техніки та захисту інформації комплексно, тобто як програмній, так і апаратній складовій. Саме це дозволить організувати максимально безпечне для підприємства інформаційне середовище. Застосування найпростіших превентивних заходів та обов'язкове регулярне проведення інвентаризації із глибинною перевіркою усіх вузлів дозволить мінімізувати загрози інформаційній безпеці суб'єкта господарювання.