

бухгалтерського проведення проводиться лише частково у вигляді “одностороннього червоного сторно” Тобто коригують не все проведення, а лише якусь його частину (або дебет або кредит) в залежності від суті зловживання.

Підсумовуючи інформацію про зловживання, які фіксують в аналітичних і синтетичних реєстрах бухгалтерського обліку необхідно назвати наступні найбільш типові:

- складання фіктивних бухгалтерських проведеннь, які не підтверджені первинними чи зведеними документами;
- складання бухгалтерських проведеннь з кореспонденцією рахунків, яка не відповідає економічному змісту операцій;
- складання коригуючих бухгалтерських проведеннь без реальної необхідності в цьому;
- використання незаконного методу виправлення бухгалтерських проведеннь в іншому календарному періоді тощо.

Зазначену вище інформацію доцільно окремо зафіксувати в чинній Інструкції, як таку, що відображає особливості експертного дослідження саме в умовах судово-бухгалтерської експертизи.

#### **Література:**

1. Закон України «Про судову експертизу». Затверджений постановою Верховної Ради України від 25.02.1994р. №4038 – XII. (зі змінами і доповненнями).
2. Інструкція про призначення та проведення судових експертиз та експертних досліджень, затверджена наказом Міністерства юстиції України від 08.10.1998р. №53/5 (зі змінами і доповненнями).
3. Мумінова – Савіна Г.Г. Судово-бухгалтерська експертиза: Навч. Посібник. – К.: КНЕУ, 2003. – 202с.

*Голяш І.Д., к.е.н., доцент ТНЕУ*

## **РОЛЬ ТА ПРИЗНАЧЕННЯ АУДИТУ ДЛЯ ПОСИЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВА**

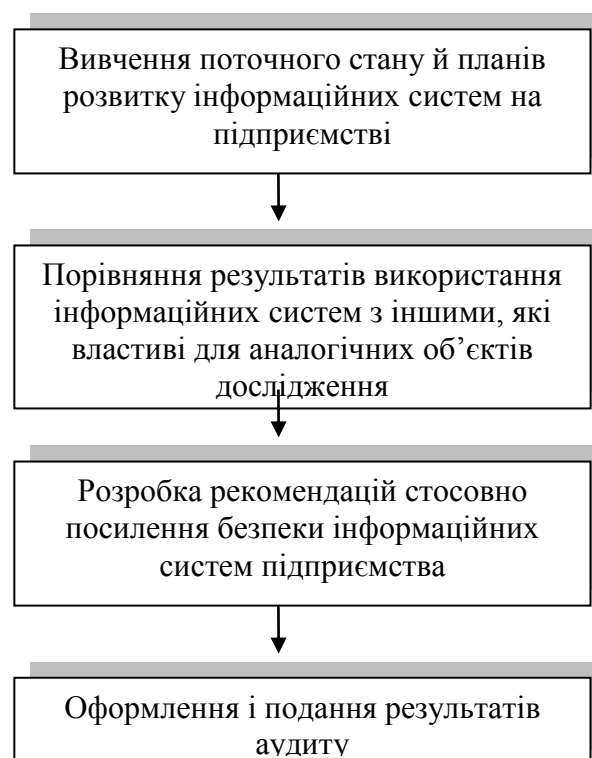
У сучасних умовах традиційний аудит не задовольняє потреб підприємств, оскільки він, зазвичай, обмежується проведенням незалежної

експертизи фінансових звітів та іншої інформації про фінансово-господарську діяльність підприємства. Тому виникає необхідність впровадження аудиту у нові сфери, зокрема у сферу інформаційних технологій, що дасть змогу вдосконалити систему захисту інформації підприємства, впровадити нові і підвищити ефективність існуючих механізмів безпеки його інформаційних систем і, як наслідок, покращити надійність функціонування підприємства.

На даний час значення аудиту для посилення безпеки інформаційних систем підприємства залишається недостатньо обґрунтованим, що є однією з причин виникнення ряду проблем на мікрорівні. Проте ми вважаємо, що аудит здатний стати реальним засобом ліквідації загроз його інформаційним системам.

На кожному підприємстві система захисту має бути цілком індивідуальною. Її повнота та дієвість залежать від існуючої законодавчої бази, від обсягу матеріально-технічних та фінансових ресурсів, виділених керівниками підприємств, від розуміння кожним з працівників важливості посилення безпеки його інформаційних систем.

Адекватність аудиту залежить від процедури та логіки побудови моделі перевірки. Організація аудиту повинна здійснюватися із врахуванням вимог підприємства стосовно посилення його безпеки інформаційних систем. Нами запропонована модель організації аудиту, яка передбачає дотримання послідовності визначених етапів для посилення безпеки інформаційних систем підприємства (див.рис.1).



## **Рис. 1. Модель організації аудиту безпеки інформаційних систем підприємства**

Як свідчить рисунок 1, поетапне проведення аудиту створює можливості для вивчення поточного стану й планів розвитку інформаційних систем на підприємстві, порівняння результатів використання інформаційних систем з аналогічними, розробки рекомендацій для підприємства стосовно посилення безпеки інформаційних систем підприємства, а також оформлення і подання результатів аудиту. Розглянута послідовність проведення аудиту є важливим елементом організації такої перевірки та служить основою для посилення безпеки діяльності підприємства. Ми вважаємо, що такий підхід може бути корисним для практики проведення аудиторської перевірки інформаційних систем підприємства.

Доцільним, на наш погляд, є доповнення процесу проведення аудиту етапом супроводу. Його потреба продиктована необхідністю періодичного консультування підприємства стосовно впровадження у практику рекомендацій експертів, внесення необхідних коригувань у їх рекомендації тощо.

Аудит безпеки інформаційних систем підприємства базується на аналізі ризику. Спираючись на методи аналізу ризику, аудитор визначає для обстежуваної інформаційної системи індивідуальний набір вимог безпеки, що найбільшою мірою враховує особливості даної інформаційної системи, середовища її функціонування і загроз безпеці, що існують в даному середовищі. Цей підхід є найбільш трудомістким і вимагає найвищої кваліфікації аудитора. На якість результатів аудиту, в цьому випадку, сильно впливає використовувана методологія аналізу і управління ризиками.

Рекомендації, сформовані за результатами аудиту, мають стосуватися розробки системи інформаційного забезпечення робочих місць, встановлення схем обміну інформації, створення контролю за роботою програмного забезпечення та його користувачами, повторного контролю змін у програмному забезпеченні, здійснення заходів щодо збереження конфіденційності даних тощо. Пропозиції повинні бути узагальнені у підсумкових документах та мають сприяти вдосконаленню системи захисту інформації, впровадженню нових і підвищенню ефективності існуючих механізмів безпеки інформаційних систем підприємства.

### **Література:**

1. Бородюк В. П. Повышение экономической эффективности системы информационной безопасности / В.П. Бородюк, А.В.Львова // Вестник МЭИ. – 2007. – №4. – С.139-142.

2. Подольский В.И. Компьютерный аудит: [Практ. пособие] / В.И.Подольский, Н.С., Щербакова, В.Л.Комиссарова; под. ред. проф. В.И.Подольского. – М.: ЮНИТИ-ДАНА, 2004. – 128с.
3. Гришина Н. В. Организация комплексной системы защиты информации./ Н.В. Гришина.– М.: Гелиос АРВ. – 2007. – 256 с.
4. Голубев В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубев [та ін]; заг. ред. Р. А. Калюжний; Гуманітарний ун-т "Запорізький ін-т держ. та муніципального управління". – Запоріжжя: Просвіта. – 2001. – С. 236-246.
5. Porter V., Hatherly D., Simon Jon. Principles of External Auditing. 3rd edition. – Wiley, 2008. – 816 p.
6. Smieliauskas W., Bewley K. Auditing: An International Approach. – McGraw-Hill Ryerson Higher Education. 2006. – 800 p.