УДК 657

Голяш І.Д., к.е.н., доц.
Саченко С.І., к.е.н., доц.
Тернопільський національний економічний університет

АУДИТ БЕЗПЕКИ ПІДПРИЄМСТВА У СФЕРІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Визначено проблеми, які стосуються безпеки підприємства у сфері застосування інформаційних технологій. Підтверджено необхідність використання аудиту для посилення такої безпеки. Визначено основні етапи аудиту у сфері застосування інформаційних технологій. Запропоновано використання результатів аудиту для вдосконалення системи захисту інформації підприємства, впровадження нових і підвищення ефективності існуючих механізмів безпеки його інформаційних систем

Визначення проблем та мети дослідження. На даний час інформація є одним із найважливіших ресурсів підприємства. Вона може бути як засобом досягнення безпеки, так і загрозою та небезпекою для підприємства.

Із розвитком інформаційних технологій стрімко зростає ризик просочування інформації, зовнішнього втручання в роботу інформаційно-телекомунікаційної системи, зараження вірусами. При цьому важливо усвідомлювати стан захищеності цінних ресурсів для того, щоб протистояти зовнішнім і внутрішнім загрозам її безпеки [1]. Пошук шляхів розв'язання наявних проблем повинен здійснюватись не тільки силами самого підприємства, але й при допомозі зовнішніх консультантів, зокрема аудиторів. Тому реальну допомогу може надати незалежне аудиторське дослідження.

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. Важлива роль у цьому напрямі належить аудиту безпеки підприємства, який стає все більш затребуваним на ринку інформаційної безпеки.

На даний час проблеми посилення безпеки підприємства у сфері інформаційних технологій розглядаються фахівцями кількох галузей знань. Такі дослідження ускладнюються тим, що потребують одночасної компетентності дослідників як в аудиті, так і в сучасних інформаційних системах і технологіях. Тому ними займаються небагато науковців і практиків. Необхідність поглиблення теоретичних та організаційно-методичних розробок у вирішенні проблем посилення безпеки підприємства у сфері інформаційних технологій та забезпечення її утримання на належному рівні, визначили мету нашого дослідження.

Особливості проведення аудиту для посилення безпеки підприємства у сфері інформаційних технологій. Тривалий час розуміння ролі аудиту для безпеки діяльності підприємства зводилося до безпеки інформації та значно звужувало її сутність [2,4]. На наш погляд, аудит є надзвичайно важливим чинником посилення безпеки підприємства, оскільки він дає змогу одержати об'єктивні якісні і кількісні оцінки поточного стану діяльності підприємства в сфері застосування інформаційних технологій.

Виділимо найпоширеніші види загроз безпеці діяльності підприємства у сфері інформаційних технологій:

– відсутність регламентованого доступу до файлів даних;
– вільне втручання в програмне забезпечення;
– відсутність протоколювання змін у програмному забезпеченні;
– відсутність регламентації користувачів інформації;
– відсутність дублювання важливих документів на документальних носіях даних;
– часті удосконалення одного і того ж програмного забезпечення різними особами;
– відсутність схем інформаційного забезпечення рівнів управління;
– наявність непідзвітних посадових осіб в системі управління, тощо [3,4,5,6].

В умовах зростаючих темпів розвитку бізнесу проведення аудиту безпеки підприємства в сфері застосування інформаційних технологій стає усе більше необхідним. При проведенні такого аудиту спеціалісти стикаються з проблемою співставлення можливих витрат на забезпечення безпеки і вигод, що отримуються при запровадженні системи безпеки. При цьому застосовується декілька методів:

– підрахунок зниження витрат, що досягаються внаслідок застосування заходів безпеки;
– розрахунок рентабельності витрат, що передбачає оцінювання дійсної (чистої) вартості ресурсів, що захищаються [1].

Визначення витрат для посилення безпеки підприємства повинен базуватися на використанні системи показників:

1) витрат на здійснення заходу;
2) розміру відверненої шкоди;
3) розміру заподіяної шкоди;
4) ефективності здійсненого заходу (як різниця відверненої та заподіяної шкоди, поділеної на витрати на здійснення заходу).

Розрахунок витрат повинен здійснюватися за допомогою спеціальних прийомів, а їх зниження має забезпечуватися шляхом застосування науково обґрунтованих методів.

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 забезпечення безпеки у сфері застосування інформаційних технологій.

Процес аудиту безпеки підприємства у сфері застосування інформаційних технологій має здійснюватися відповідно до визначених етапів. У зв'язку з цим, ми пропонуємо модель організації аудиту, яка зображена на рис. 1.

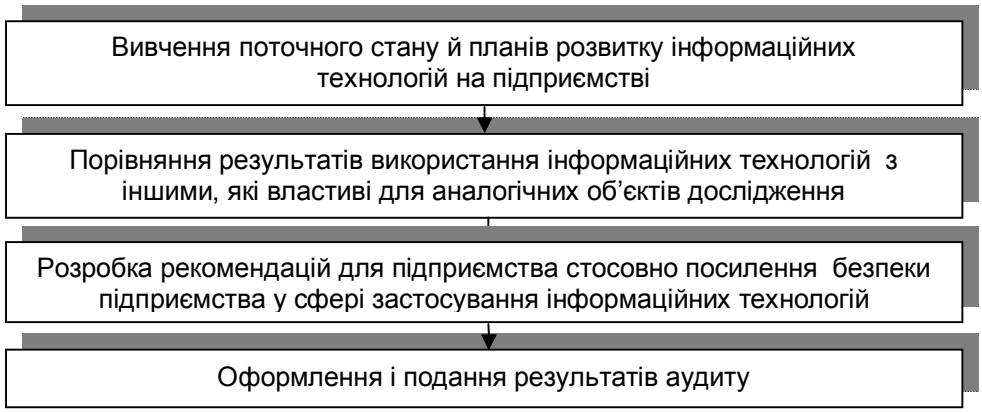

Рис. 1. *Модель організації аудиту безпеки підприємства у сфері застосування інформаційних технологій*

Як свідчить рис. 1, поетапне проведення аудиту створює можливості для вивчення поточного стану й планів розвитку інформаційних технологій на підприємстві, порівняння результатів використання інформаційних технологій з аналогічними, розробки рекомендацій для підприємства стосовно посилення безпеки підприємства у сфері застосування інформаційних технологій, 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 у сфері застосування інформаційних технологій.

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 діяльності підприємства у сфері інформаційних технологій доцільно проводити експертним шляхом. При проведенні такого аудиту виявляють недоліки в системі заходів захисту інформації на основі досвіду експертів, що беруть участь в аудиті. Мета проведення експертного аудиту полягає в оцінці стану інформаційної системи і розробці рекомендацій із застосування комплексу організаційних заходів і програмно-технічних засобів, спрямованих на захист інформаційних та інших ресурсів інформаційної системи від загроз. Експертний аудит дає змогу прийняти обґрунтовані рішення з використання засобів захисту, оптимальних щодо їх вартості й можливості попередження загроз безпеці діяльності підприємства у сфері інформаційних технологій. Такий аудит 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.

Внаслідок проведення аудиту формуються рекомендації, які спрямовані на посилення безпеки підприємства у сфері застосування інформаційних технологій. Ці рекомендації мають стосуватися таких напрямків:

– 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.

Результати аудиту безпеки підприємства у сфері інформаційних технологій мають бути узагальнені у пакеті підсумкових документів, що містять деталізовані рекомендації стосовно вдосконалення системи захисту інформації, впровадження нових і підвищення ефективності існуючих механізмів безпеки інформаційних систем.

Висновки. Необхідність поглиблення теоретичних та організаційно-методичних розробок у вирішенні проблем посилення безпеки підприємства у сфері інформаційних технологій дало змогу сформувати такі висновки:

В умовах стрімкого розвитку інформаційних технологій виникла необхідність захищеності інформаційних ресурсів підприємства для протистояння зовнішнім і внутрішнім загрозам його безпеки. З метою посилення безпеки підприємства у сфері інформаційних технологій та її утримання на належному рівні пропонується проведення незалежного аудиторського дослідження.

На даний час значення аудиту для посилення безпеки підприємства у сфері застосування інформаційних технологій 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 діяльності у сфері інформаційних технологій.

1. Проблеми посилення безпеки підприємства у сфері інформаційних технологій розглядаються фахівцями кількох галузей знань. Враховуючи підвищену зацікавленість до проблем розвитку аудиту у сфері інформаційних технологій, вважаємо, що теоретико-організаційні засади та напрямки практичного застосування цього виду аудиту вимагають подальших досліджень та глибокого вивчення.

2. Використання аудиту для посилення безпеки підприємства у сфері інформаційних технологій дозволить більш повно задовольнити потреби власників підприємств та його менеджерів, яких цікавить питання довгострокового стратегічного розвитку. Тому ми вважаємо, що такий вид аудиту повинен використовуватися для оцінки проблем поточного стану підприємства та має стати невід'ємним елементом системи його управління.

3. При проведенні аудиту спеціалісти стикаються з проблемою співставлення можливих витрат на забезпечення безпеки і вигод, що отримуються при запровадженні системи безпеки. При цьому розрахунок витрат повинен здійснюватися за допомогою спеціальних прийомів, а їх зниження має забезпечуватися шляхом застосування науково обґрунтованих методів.

4. Адекватність аудиту залежить від процедури та логіки побудови моделі перевірки. Організація аудиту повинна здійснюватися із врахуванням вимог підприємства стосовно посилення його безпеки у сфері інформаційних технологій. Нами запропонована модель організації аудиту, яка передбачає дотримання послідовності визначених нами етапів для посилення безпеки підприємства у сфері застосування інформаційних технологій. Доцільним, на наш погляд, є доповнення процесу проведення аудиту етапом супроводу. Його потреба продиктована необхідністю періодичного консультування підприємства стосовно впровадження у практику рекомендацій експертів та внесення необхідних коригувань.

5. Аудит безпеки діяльності підприємства у сфері інформаційних технологій доцільно проводити експертним шляхом. Експертний аудит дасть змогу прийняти обґрунтовані рішення з використання засобів захисту, оптимальних щодо їх вартості й можливості попередження загроз безпеці діяльності підприємства у сфері інформаційних технологій.

6. 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 пакеті підсумкових документів та мають сприяти вдосконаленню системи захисту інформації, впровадженню нових і підвищенню ефективності існуючих механізмів безпеки інформаційних систем.

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. – 128 с.

3. *Гришина Н.В.* Организация комплексной системы защиты информации./ Н.В. Гришина.– М.: Гелиос АРВ. – 2007. – 256 с.

4. *Голубєв В.О.* Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В.О. Голубєв [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 B., 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.

ГОЛЯШ Ірина Дмитрівна – кандидат економічних наук, доцент кафедри аудиту, ревізії та контролінгу Тернопільського національного економічного університету.

САЧЕНКО Світлана Іванівна – кандидат економічних наук, доцент кафедри аудиту, ревізії та контролінгу Тернопільського національного економічного університету.

Стаття надійшла до редакції 04.01.12 р.