тратах протягом короткого планового періоду. У динамічній моделі обліку це невизначені умови формування попиту і пропозиції [2, с.16].

У сучасних умовах бухгалтер повинен знати різні методи формування фінансових результатів, уміти вибрати і запропонувати керівництву той варіант облікової політики, який забезпечить реалізацію прийнятої на підприємстві фінансової стратегії. Отже, сфера діяльності бухгалтера значно розширюється – від ведення бухгалтерського обліку до фінансового менеджменту.

Література:

1. Голов С. Ф. Бухгалтерський облік за міжнародними стандартами: приклади та коментарі
2. Гуцаленко Л.В. Адаптивна система обліку і контролю результатів діяльності сільськогосподарських підприємств: монографія / Гуцаленко Л.В. –К: ННЦ ІАЕ, 2010.- 372 с.

***Ірина Данилюк**, к.е.н.,доцент*
***Владислав Данилюк**, студент*
Тернопільський національний економічний університет
м. Тернопіль, Україна

АУДИТОРСЬКА ОЦІНКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

Тенденцією нашого часу стає поглиблення розуміння Всесвіту як інформаційної системи, що насичена різноманітними за змістом потоками символів, повідомлень та іншими інформаційними складовими.

Революція в науково-технічній сфері призвела до появи нових видів інформаційно-комунікаційних технологій, що стали матеріальним підґрунтям глобалізаційних процесів. Інформатизація усіх сфер життєдіяльності змінила розуміння сутності феномену безпеки, джерел та характер загроз, значення та роль міжнародних інституцій.

Становлення інформаційного суспільства має як безсумнівні позитивні, так і певні негативні наслідки. З одного боку, прискорилася передача інформації значного обсягу,її обробка та впровадження. З іншого – серйозне занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з архівів, банків та баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо.

Перехід до інформаційного суспільства змінив статус інформації. Наразі, вона може бути як засобом досягнення безпеки, так і загрозою та небезпекою для підприємства.

Тривалий час розуміння аудиту інформаційної безпеки в наукових джерелах ототожнювалося тільки з безпекою інформації, що значно звужувало її сутність. Саме тому з низки питань, присвячених розгляду проблеми інформаційної безпеки підприємств, найбільш вивченими та дослідженими її аспектами є безпека інформації (інформаційно-технічна безпека, в нашому розумінні).

Проблема розробки систем аудиту інформаційної безпеки у вітчизняній науковій літературі ґрунтовно не досліджувалася, а розглядалася лише через висвітлення окремих її аспектів вітчизняними та зарубіжними фахівцями. У цьому контексті слід згадати наукові розробки таких вчених як В. Артемов, І. Бачило, К. Бєляков, В. Богуш, В. Брижко, В. Гавловський, В. Голубєв, В. Горобцов, С. Комов, Н. Кушакова, А. Марущак, В. Петренко, В. Цимбалюк, І. Чиж, В. Ярочкін та інші.

Аудит безпеки дозволяє перевірити, наскільки добре захищена інформаційна система підприємства від внутрішніх і зовнішніх загроз. Регулярний аудит дозволяє підтримувати систему інформаційної безпеки на належному рівні, вчасно виявляти потенційні проблеми, контролювати дотримання правил і норм політики безпеки, на підприємстві.

Тестування на проникнення – є одним з видів аудиту інформаційної безпеки, що дозволяє виявити зовнішні загрози, до яких схильні Інтернет-ресурси підприємства. В ході аудиту проводять комплексне обстеження серверів, підключених до мережі Інтернет, виявляють уразливі місця і помилки конфігурації при використанні яких можна проникнути на сервер ззовні й отримати несанкціонований доступ до критичної інформації порушити її цілісність і доступність.

Внутрішній аудит інформаційної безпеки вимагає фізичної присутності аудиторів на досліджуваному об’єкті, коли фахівці проводять співбесіду з керівниками підприємства різних рівнів, вивчають специфіку бізнес-процесів підприємства, структуру інформаційної системи, правила розмежування доступу, існуючу внутрішню документацію, яка регламентує правила і норми роботи з конфіденційною інформацією. Проводять тестування захищеності інформаційної системи від внутрішніх загроз (включаючи людський фактор), перевіряють налаштування серверів і комп’ютерних робочих місць підприємства, перелік дозволеного до використання програмного забезпечення, наявність оновлень і патчів, ефективність роботи захисних засобів – антивірусів, міжмережевих екранів, антишпіонских програм та ін. Перевіряють політику резервного копіювання, методи зберігання інформації та її захищеності від непередбачених втручань.

Аудитор повинен використовувати рекомендації міжнародних стандартів у поєднанні з власними методиками, розробленими протягом років роботи і постійно їх удосконалюватись з урахуванням сучасних реалій і загроз. Частина робіт із зовнішнього аудиту повинна бути автоматизованою за допомогою новітніх продуктів виробництва, що дозволить за короткий час перевірити систему на стійкість до десятків тисяч відомих атак. Іншу, більш складну частину робіт можна виконувати вручну із застосуванням досвіду та знань експертів для здійснення безпечних проникнень у досліджувані системи і для вироблення рекомендацій та інструкцій щодо усунення виявлених вразливостей систем захисту.

Можна виділити такі основні види аудиту інформаційної безпеки:

- експертний аудит безпеки, в процесі якого виявляють недоліки в системі заходів захисту інформації на основі наявного досвіду експертів, що беруть участь в процедурі обстеження;
- оцінка відповідності рекомендаціям Міжнародних стандартів;
- інструментальний аналіз захищеності АС, спрямований на виявлення і усунення недоліків програмно-апаратного забезпечення системи;
- комплексний аудит, що включає всі вище наведені форми обстежень.

Кожний із видів аудиту проводитись окремо або в комплексі, залежно від тих завдань, які необхідно вирішити підприємству. Об'єкт аудиту може виступати АС компанії в цілому та і її окремі сегменти, в яких проводиться обробка інформації [2; с. 244].

Аудит інформаційної безпеки – це системний процес здобуття неупереджених високоякісних і кількісних оцінок поточного стану корпоративної інформаційної системи в узгодженні з певними аспектами інформаційної безпеки.

Важливим елементом розвитку сучасних підприємств є автоматизація бізнес-процесів з впровадженням засобів обчислювальної техніки і телекомунікацій. Наслідком цього є неухильне збільшення розмірів інформації, яка піддається обробці і скупченню в електронному вигляді.

Наслідком електронного документообігу підприємства є залежність його діяльності від безперервності функціонування інформаційної системи (ІС) як одного цілого і від збереження корпоративної інформації в процесі її обробки та збереження на електронних носіях.

Але варто пам'ятати, що існує можливість відмови устаткування, що призводить до збоїв у доступі до електронної інформації, а в гіршому випадку – до вибіркової або абсолютної її втрати. Відомі випадки, коли простій інформаційної системи приводив до фінансових збитків, які неодноразово перевищують ціну самої системи.

Зростання інформаційної системи підприємства, що є неминучим наслідком вдалого розвитку бізнесу, має на меті посилення вимог до безпе-

рервності її функціонування, а також до збереження і конфіденційного використання корпоративної інформації. ІС підприємства перетворилася з друкарської машини в інструмент ведення бізнесу, що, у свою чергу, втягує підприємство у залежність від уразливості.

Однією з критичних якостей уразливості ІС є недоступність плану заходів щодо відновлення її працездатності після кризи. У разі виникнення форс-мажорних подій можна орендувати будівлю, купити техніку, підключити телекомунікації, але неможливо повернути функціональність ІС, якщо втрачена інформація із спеціального джерела її обробки.

Результати аудиту дозволяють створити кращу за ефективність і витратами систему захисту корпоративної інформації, адекватну поточним завданням і цілям бізнесу.

Принципово усвідомлювати і обдумувати те, що:

- досягнення інформаційної безпеки є безперервним процесом, пов'язаним з правовими, організаційними і програмно-апаратними заходами захисту;

- в основі цього процесу лежить періодичний аналіз безпеки інформаційної системи в розрізі небезпек і динаміки їх розвитку;

- інформаційна система, у власному розвитку, зобов'язана піддаватися періодичним реорганізаціям, відправним моментом будь-якого з них має бути тест виявлених недоліків під час виконання аудиту інформаційної безпеки.

Аудит інформаційної безпеки зобов'язаний бути націлений як на професіоналів в галузі ІТ-безпечності, так і на фахівців в галузі менеджменту. Така вимога позбавляє появи непорозуміння фахівців в галузі інформаційної безпеки ТОР-менеджерами компанії.

Для перевірок ефективності й безпечності інформаційної системи як такої здійснюють комп'ютерний аудит інформаційної системи. Під ним мається на увазі оцінка поточного стану комп'ютерної системи на відповідність певному стандарту або запропонованим вимогам [11, с. 259]. Цей термін використовується насамперед спеціалістами з загальної безпеки комп'ютерних інформаційних систем і у вузькому значенні не стосується аудиту фінансової звітності. Такий аудит не спрямований на висловлення конкретного рішення, він дає можливість поглянути на інформаційну систему комплексно, виявити проблемні місця, сформувати обґрунтовані рекомендації для ухвалення рішення про усунення недоліків і включає декілька напрямів (рис. 1).

Аудит ефективності інформаційної системи дає можливість підприємству оцінити сукупну вартість інформаційної системи і порівняти показники досліджуваної системи з лідером у цій галузі, а також оцінити терміни повернення інвестицій при вкладенні коштів в інформаційну систему, розробити

оптимальний варіант вкладень, визначити обсяг коштів на обслуговування й підтримку системи, знизити виробничі витрати. Цей вид аудиту включає такі частини інформаційної системи підприємства як апаратні засоби, програмне забезпечення, периферійні пристрої, ІТ-персонал компанії, а також документи, бізнес-процеси, інформаційні потоки, користувачів.

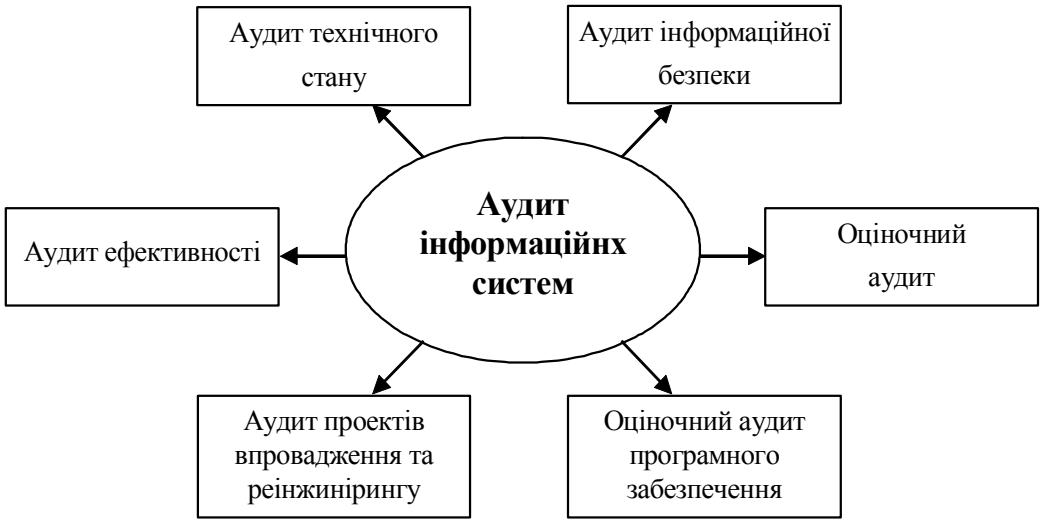

Рис. 1. Напрями аудиту інформаційних систем

Здебільшого комп'ютерний аудит інформаційних систем потрібний, якщо автоматизована система призначена для обробки конфіденційної чи секретної інформації. Але саме до таких належать комп'ютерні системи фінансового обліку. Проведення комп'ютерного аудиту корисно також після побудови автоматизованої системи та її підсистеми безпеки на етапі приймання в експлуатацію для оцінки ступеня дотримання висунутих до неї вимог [4; с. 159].

Отже, аудит інформаційної безпеки – це системний процес отримання неупереджених високоякісних і кількісних оцінок поточного стану корпоративної інформаційної системи з узгодженням певних аспектів захисту, основними завданнями якого є справедлива оцінка поточного стану інформаційної безпеки компанії, а також її адекватність цілям і задачам бізнесустосовно збільшення ефективності і рентабельності фінансової діяльності компанії.

Література:

1. Аглицький І.В. Інформаційні технології і бізнес: навчальний посібник./ І.В. Аглицький – К.: Знання, 2002. – 341 с.
2. Бутинець Ф.Ф. Аудит: стан і тенденції розвитку в Україні та світі: моногр. / За ред. проф. Ф.Ф. Бутинень, Н.М. Малюга, Н.І. Петренко – Житомир: ЖДТУ, 2004. – 564 с.
3. Завгородній В.П. Автоматизація бухгалтерського обліку, контролю, аналізу та аудиту. / В.П. Завгородній – К.: А.С.К., 2004. – 768 с.

4. Івахненков С.В. Комп'ютерний аудит: контрольні методики і технології: наукове видання. / С.В. Івахненков – К.: Знання, 2005. – 286 с.
5. Клименко О.В Інформаційні системи і технології в обліку: навчальний посібник. / О.В. Клименко К: Центр учбової літератури, 2008. – 320 с.
6. Кондрашова С.С. Інформаційні технології в управлінні: учбовий посібник/ С.С. Кондрашова К.: МАУП. 2007.-250 с.
7. Крилов І. В. Інформаційні технології: теорія і практика: учбовий посібник. / І.В. Крилов М.: Центр, 2006.-530 с.
1. 8.Петрик В.М. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: навчальний посібник. / В.М. Петрик, В.В. Остроухов та ін. – К.: Росава, 2006. – 208 с.
2. 9.Сухоруков А.І. Пріоритети інвестування інформаційно-технологічного розвитку / А.І. Сухоруков // Стратегічна панорама. - 2008.-№1.- 150с.
10. Чубатенко О.І. Інформаційні технології – майбутнє України . / О.І. Чубатенко // Дзеркало тижня.-2007.-№1.
11. Щербакова Н.С. Аудит інформаційної безпеки: навч. посіб. / Н.С. Щербакова – Харків: Ескада, 2004. – 328 с.
12. Weber R. Information systems control and audit. – Upper Saddle River, Prentice-Hall, Inc., 2001. – 1013 p.

Василь Дерій, *к.е.н., доцент*
Тернопільський національний економічний університет
м. Тернопіль, Україна

ФОРМУВАННЯ СЕРЕДОВИЩА КОНКУРЕНТОЗДАТНОСТІ ПІДПРИЄМСТВ І КОНТРОЛЬ ЗА ВИТРАТАМИ ТА ДОХОДАМИ В ЦИХ УМОВАХ

У сучасному глобалізованому світі, ні одне підприємство немає суттєвих шансів на виживання, якщо воно не приділятиме належної уваги проблемам своєї конкурентоздатності. Правда, за нашим переконанням, проблеми конкурентоздатності вітчизняних підприємств необхідно, водночас, вирішувати на макро-, мезо- і макрорівнях з розробкою та узгодженням відповідних планів, програм, зміцненням конкурентоздатності країни, галузі, комплексу, регіону, підприємства на певний календарний рік чи кілька календарних років (періодів).