004.056: 330

Спільна Н.П., к.е.н., професор,
Одеська національна академія зв'язку імені О.С. Попова,
Махновська Н.Д., к.е.н., викладач,
Одеський національний університет імені І.І. Мечникова

МЕТОДОЛОГІЧНИЙ ПІДХІД ДО ОЦІНКИ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ

З розвитком і ускладненням засобів, методів і процесів обробки інформації підвищується залежність сучасного суспільства від ступеня безпеки використовуваних їм інформаційних технологій. Незважаючи на закони України «Про інформацію» [1], «Про захист інформації в інформаційно-телекомунікаційних системах» [2], «Про авторське право й суміжні права» і «Про поширення екземплярів аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних», нелегальне копіювання, комп'ютерні диверсії (віруси, «бомби», «трояни»), а також кількість фінансових злочинів з використанням обчислювальної техніки не зменшується [3]. Тому захист інформації (ЗІ) є однією з найважливіших проблем інформаційних технологій.

На сьогоднішній день значна увага приділяється вивченню цієї проблеми з технічного та економічного напрямку, а також вкладаються значні інвестиції. Фахівці технічного профілю здійснюють розробку систем захисту інформації (СЗІ) та проводять роз'яснюючу інформаційну роботу з клієнтами. Завдання економістів розрахувати економічну ефективність використання цих систем на підприємствах з урахуванням форм власності та партнерських відносин.

Окремі проблеми та особливості захисту інформації досліджували різні вчені, зокрема: В. Герасименко, В. Домарєв, Д. Зегжда, Г. Конахович, А. Малюк, С. Петренко, С. Расторгуєв, О. Редькін, Ю. Уфімцев, П. Хорєв, В. Хорошко, В. Шорошев. Значний внесок у розвиток цих проблем належить зарубіжним вченим Н. Вінеру, Д. Сяо, Б. Ролкеру, Л. Дж. Хоффману, К. Шеннону.

В роботах цих та багатьох інших вчених напрацьовано достатньо науково-теоретичного та методичного матеріал, запропоновано безліч різноманітних практичних рекомендацій щодо розв'язання тих чи інших питань, вирішення прикладних завдань, які не втратили своєї актуальності й донині, а саме: абсолютний захист створити не можна; система захисту інформації повинна бути комплексною; СЗІ повинна адаптуватись до мінливих умов. Разом з тим, аналіз опублікованих праць з даної проблематики дає підстави говорити, що в цілому дослідження зосереджені на формуванні стандартних процедур захисту інформації. Недостатньо науково розкритою залишається оцінка ефективності інформаційної безпеки. З цих позицій, формування методичних підходів до розрахунку економічної ефективності захисту інформації та автоматизація розрахунків є необхідним та актуальним.

Таким чином, мета статті полягає в обґрунтуванні теоретичних та методичних підходів щодо розрахунку економічної ефективності захисту інформації підприємств різної форми власності, аналізі систем захисту інформації, автоматизація представлених розрахунків.

В даний час всі провідні західні країни і Україна, в тому числі, підіймаються на новий етап розвитку – етап інформаційного суспільства, коли сумарна вартість інформації та інформаційних технологій, що використовуються в суспільстві перевищує витрати на інші види діяльності. Інформація та інформаційні технології стають основним ринковим товаром у суспільстві. Тому найбільш важливими складовими об'єкта захисту є інформація і засоби обробки і зберігання інформації.

Головною відмінністю інформаційної інфраструктури, як об'єкта захисту, є те, що вона має розподілений характер, охоплюючи практично всі компоненти організації. Все це істотно ускладнює забезпечення безпеки об'єкта обробки інформації.

Для протистояння процесу порушення безпеки необхідно виділити однорідні елементи захисту. Оскільки вони забезпечують однотипність засобів використовуваних для протидії загрозам, то необхідно зробити системну класифікацію процесів забезпечення захищеності, виділивши в ньому однорідні підпроцеси. Сучасні системи безпеки ґрунтуються на реалізації комплексу заходів щодо організації захисту інформації (рис. 1).

Як показали дослідження проблема оцінки ефективності захисту інформації досить широка і включає технічні, економічні, організаційні й інші аспекти. Тому вважаємо, що для оцінки

ефективності інформаційної захищеності в межах підприємств необхідно виділити відповідні показники.

Рис. 1. Основні напрямки комплексного захисту інформації

При оцінці забезпечення захисту інформації у межах підприємств можна виділити такі показники:

− економічні (слугують для оцінки економічної ефективності);

− організаційні (визначають міру інтеграції нової інформаційної системи з існуючою, а також дозволяють оцінити якість ІТ-проекту);

− комерційні (характеризують ефективність проведення програми реалізації і просування інформаційних систем та Інтернет-технологій у межах підприємства та ефективність їх використання).

Економічна доцільність характеризується обґрунтуванням техніко-економічних методів і засобів, що дозволяють кількісно виміряти ефективність витрат на захист інформації. Серед основних показників ефективності ЗІ є: сукупна вартість володіння; економічна ефективність бізнесу; коефіцієнт повернення інвестицій та інші [4]. На основі аналізу таких факторів як: політика безпеки, організація захисту, управління персоналом, фізичної безпеки, доступу до систем, відповідність вимогам ЗІ необхідно побудувати оптимальний алгоритм автоматизації ЗІ. Для обґрунтування результату від поетапної реалізації необхідно врахувати максимальне зниження сукупних витрат [5].

При організації захисту інформації виділяємо наступні витрати:

− витрати на первинний аналіз і планування;

− вартість необхідного устаткування;

− вартість програмного забезпечення;

− вкладення в організацію ліній зв’язку і супутнє устаткування;

− витрати на підготовку та перепідготовку кадрів;

− вартість допоміжного устаткування, наприклад комп’ютерної техніки, необхідної для оновлення інформації на Інтернет-сайті або для виконання функцій із забезпечення працездатності інформаційних технологій;

− витрати, пов’язані з експлуатацією технічної частини електронної системи;

− заробітна плата обслуговуючого персоналу;

− витрати на допоміжні матеріали;

− оплата провайдерам різних послуг Інтернету;

− амортизаційні відрахування;

− додаткові витрати у разі залучення сторонніх підприємств до робіт з розвитку інформаційних систем;

− витрати на рекламні кампанії, що проводяться;

− витрати, обумовлені недостовірністю обробки інформації;

− витрати, викликані відмовами у роботі технічної частини системи.

Далі можна використовувати методику аналізу економічної доцільності захисту інформації при зміні форми власності підприємств (рис. 2).

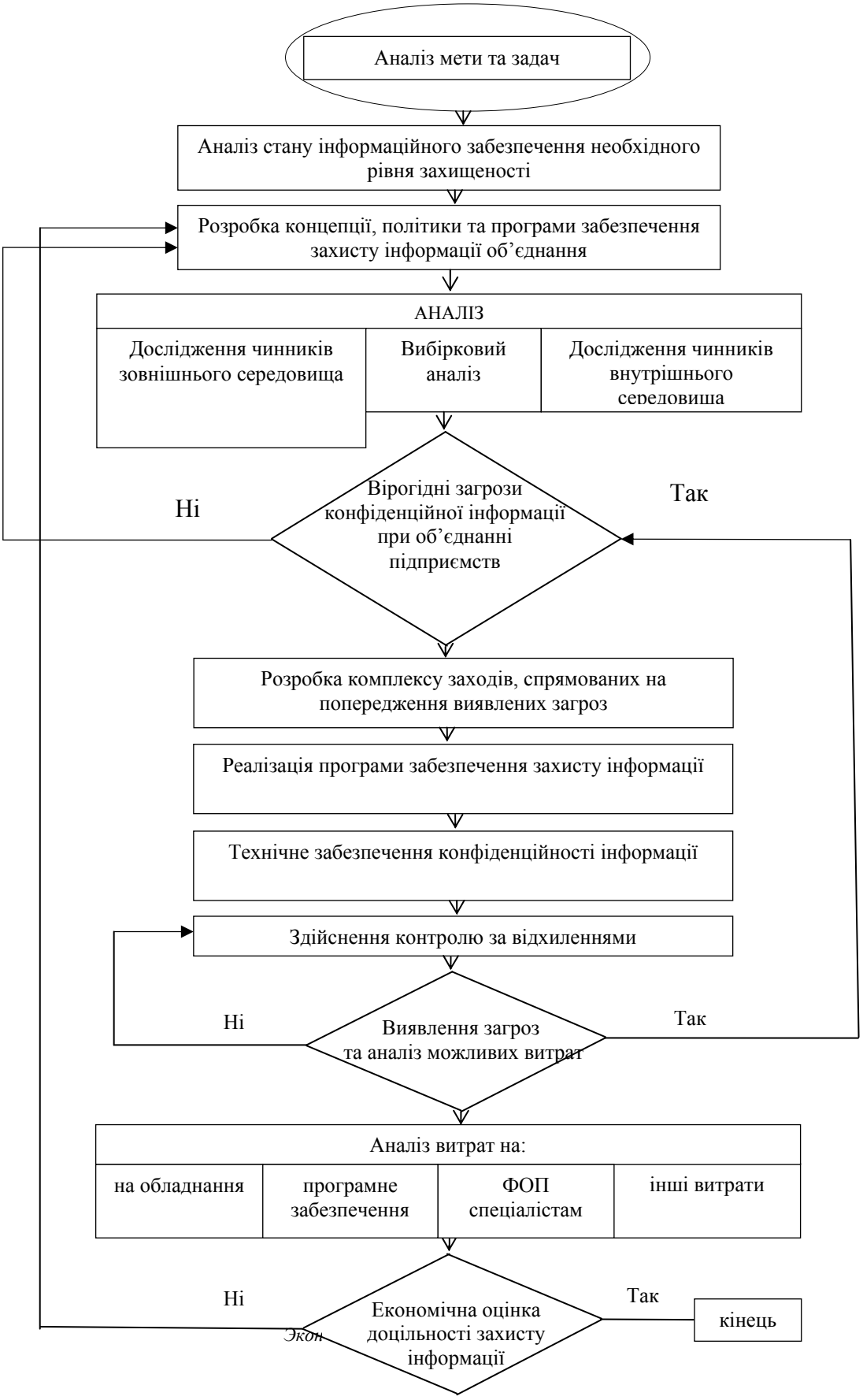

Рис. 2. Алгоритм аналізу ефективності захисту інформації

Застосування алгоритму аналізу ефективності захисту інформації дає можливість аналізувати витрати. Тобто система буде ефективною у тому випадку, якщо витрати на її створення будуть меншими за витрати внаслідок знищення або блокування інформації, її несанкціонованого витоку. Вартість засобів забезпечення ЗІ має відповідати ризику і прибутку, тобто вкладання коштів у СЗІ мають показати скорочення можливих втрат від реалізації загроз. Розробка концепції, політики та програми ЗІ повинна визначати обсяг інвестицій у напрямку найбільшої уразливості.

Як показали дослідження, найбільш ризиконебезпечним і витратним є процес бухгалтерського обліку. Одна помилка може викривити інформацію про фінансовий та майновий стан підприємства, установи чи організації. В сучасних умовах, що характеризуються швидкими темпами розвитку комп'ютерних технологій, роль та цінність облікової інформації особливо зростає. При налагодженні та функціонуванні комп'ютерних систем, частина облікової інформації стає доступною для сторонніх осіб. Тому слід за допомогою особливих внутрішніх положень (наказів, інструкцій) обмежити доступ сторонніх осіб до інформації, яка є комерційною таємницею підприємства, а також встановити або передбачити механізм перевірки звітної інформації, що виходить за межі підприємства.

Досвід комп'ютеризації обліку на підприємствах дозволяє виділити дві передумови, характерні для організації комп'ютеризованого обліку:

– наявність грошових коштів для інвестицій у створення та експлуатацію інформаційної системи (80 % невдач у комп'ютеризації обліку зумовлені відсутністю коштів);

– зацікавленість керівництва підприємства у впровадженні інформаційних систем (на шляху комп'ютеризації обліку, як показали дослідження, через незацікавленість керівництва зазнали невдач близько 20 % підприємств).

Створення комп'ютерних систем обліку має базуватися на таких основних принципах:

– економічна доцільність (переваги, що очікуються від використання системи, мають перевищувати витрати на проектування, впровадження, навчання, супровід);

– контроль (створення паралельних інформаційних потоків, що контролюють один одного та забезпечують достовірність облікових даних);

– гнучкість (система, що створюється, повинна мати достатній запас гнучкості, щоб забезпечити можливість реагування на зміну зовнішніх факторів);

– сумісність (систему слід проектувати з урахуванням людського фактора та організаційних особливостей підприємства, вже наявних комп'ютерів і програм);

– універсальність (програмна система має вирішувати не окреме завдання, а виконувати стандартні процедури й обробляти конкретне завдання як окремий випадок більш загального);

– системний підхід(введення інформації в систему і багатократне її використання);

– надійність (забезпечується різними способами, наприклад, дублюванням структурних елементів системи або їхньою надлишковістю);

– моделювання (побудова моделі програмного засобу, що описує основні особливості інформаційно-логічної структури системи обробки облікових даних, правила її функціонування й адаптації до потреб користувача);

– захист і безпека даних (система, що проектується, має сприяти захисту активів підприємства від нераціонального їх використання і забезпечувати надійність та безпеку інформації в системі.

Якісна комп'ютеризована система бухгалтерського обліку має виконувати такі функції щодо безпеки даних: 1) поділ доступу до функцій і даних системи шляхом авторизації користувачів за паролем; 2) шифрування даних; 3) наявність контролю за входом до системи і ведення журналу робочого часу; 4) контроль за періодичністю створення резервних (архівних) копій інформації [6, 7].

Бухгалтерська інформаційна система об'єднання підприємств має забезпечувати: автоматизоване вирішення всього комплексу завдань бухгалтерського обліку, планування, аналізу фінансово-господарської діяльності підприємства, а також внутрішнього контролю; одержання оперативної інформації, що постійно змінюється, про поточний стан справ на підприємстві. Такий режим важливий, наприклад, для підприємств зв'язку, які намагаються більш ефективно використовувати свої ресурси, а також для інших підприємств, де відбувається постійний рух великих обсягів коштів.

Об'єднання підприємств можуть мати філії або склади, які розміщені географічно відокремлено. Крім того, такі підприємства можуть належати групі власників. Тому актуальним є наявність в комп'ютерних системах обліку КСБО робочих місць з можливістю здійснювати обмін даними для оперативного управління із центру для ефективного захисту інформації.

В процесі оцінки ефективності необхідно використовувати міжнародний стандарт управління інформаційною безпекою ISO 17799: 2000, в якому відображені основні поняття та методика якісної оцінки рівня захищеності інформаційної системи [8]. Оцінюється відповідність системи певному класу, рівню захищеності чи певному стандарту безпеки. Позитивними сторонами є виявлення основних загроз безпеки для бізнес-процесів, розробка рекомендацій для підвищення поточного рівня захищеності облікової інформації. Таким чином, розробка методичних підходів щодо розрахунку економічної ефективності захисту інформації підприємств різної форми власності є важливим кроком, тому що це сприяє скороченню витрат для отримання необхідної інформації, надає більшу ефективність передачі даних, точність і достовірність.

Аналіз використовуваних захисних методів і заходів свідчить, що їх реалізація для кожного підприємства різна, відповідно і ефективність таких заходів для одних об'єктів вища (холдинги, кластери, фінансово- промислові групи), а для інших нижча (об'єкти малого бізнесу). Результати дослідження можуть бути використані при підготовці фахівців з питань захисту інформації, або при розробці комплексних систем захисту інформації для підприємств різної форми власності.

Література

1. Закон України «Про інформацію» від 02.10.1992// Відомості Верховної Ради України, 1992, № 48(01.12.1992)

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994, 20.05.1999 // Відомості Верховної Ради України, 1994, №31 (02.08.1994)

3. Постанова КМ України № 1126 від 08.10.97р. «Концепція технічного захисту інформації в Україні» [Електронний ресурс]/ Ліга: Еліт: Мережна версія.

4. Адаховська Я.І. Методичні підходи до визначення економічної ефективності захисту інформації / Я.І. Адаховська, Т.Є. Зарицька, Н.П. Спільна // Матеріали Міжнародної науково-практичної конференції, 5-6 квітня 2012р. – Одесса: ОНАЗ ім. О.С. Попова, 2012 . – С. 95-98

5. Тардаскіна Т.М. Підходи до оцінки витрат на підтримку та створення системи інформаційної безпеки / Т.М. Тардаскіна // Інформаційні технології в економіці, менеджмент і бізнес. Проблеми науки, практики і освіти. – Київ, 2006 – Т3. – С. 286-288.

6. Голов С.Ф. Розвиток бухгалтерського обліку та аудиту відповідно до плану дій «Україна-ЄС» / С.В. Голов // Весник бухгалтера и аудитора Украины. – 2005. Тардаскіна № 15-16. – С. 10-20.

7. Петрук О.М. Нова парадигма бухгалтерського обліку / О.М. Петрук // Науково-практичний журнал. – 2003. – № 1: Полтава: Регіональні перспективи. – С. 70-72.

8. Войтко С.В. Менеджмент у телекомунікаціях: навч. посібник/ С.В. Войтко, К.П. Ангелов; за наук. ред. В.Г. Герасимчука. – К.: Знання, 2007. – С. 242-295.

338. 65. 2 (075. 8)

Ячменева В.М., д.э.н., профессор,
Кузьмич В.А., соискатель,
Национальная академия природоохранного и курортного строительства

СУЩНОСТЬ И РОЛЬ АДМИНИСТРАТИВНОГО МЕНЕДЖМЕНТА В УПРАВЛЕНИИ ПРЕДПРИЯТИЕМ

В настоящее время в Украине наблюдается активный процесс рыночных преобразований, значительный рост новых организационных форм хозяйствования. Через ошибки и опыт, через преодоление субъективных и объективных трудностей появляются новые типы организаций, как в предпринимательстве и бизнесе, так и в государственном секторе, которые уже не могут работать по-старому и остро нуждаются в специалистах и руководителях, способных решать новые сложные задачи развития, которые ставит перед ними рыночная экономика. Практически все компании и фирмы на определенном этапе сталкиваются с проблемой эффективного управления, что делает проблему разработки и развития теоретических основ административного менеджмента в нашей стране особенно актуальной. Причем это не должно сводиться к механическому перенесению