УДК 657.221:65.012.8

Дикий А.П

ПОЛІТИКА ЕКОНОМІЧНОЇ БЕЗПЕКИ В ЧАСТИНІ ЗАХИСТУ БУХГАЛТЕРСЬКОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ В УМОВАХ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Внутрішній контроль економічної безпеки підприємства передбачає здійснення процесу отримання об'єктивних, якісних та кількісних оцінок про поточний стан економічної безпеки підприємства відповідно до певних критеріїв та показників безпеки. В статті запропоновано заходи контролю, які дозволять перевіряти ступінь дотримання економічної безпеки підприємства. Результати контролю безпеки дозволяють побудувати оптимальну з точки зору ефективності та витрат систему захисту бухгалтерської інформації, адекватну поточним завданням та цілям підприємницької діяльності

Вступ. Внутрішній контроль за дотриманням економічної безпеки підприємства є одним з найбільш актуальних напрямів стратегічного та оперативного менеджменту, що динамічно розвиваються, в галузі безпеки інформації. Результати контролю безпеки дозволяють побудувати оптимальну з точки зору ефективності та витрат корпоративну систему захисту бухгалтерської інформації, адекватну поточним завданням та цілям підприємницької діяльності.

Питання економічної безпеки підприємства в частині захисту інформації знайшли своє відображення у працях ряду дослідників, серед яких: А.О. Азарова, О.В. Гаврилова [1], І.О. Александров, О.В. Половян [2], Г. Андрощук [3; 4], О.В. Ареф'єва [5], В.С. Барсуков [6], Ю.М. Батурін, А.М. Жоздішевський [7], І.В. Василевський [8], В.І. Василець, В.М. Голованов [9], В.С. Горячев [10], С.Дж. Грей, Б.Е. Нідлз [11], В. Забродський, Н. Капустін [12], Н. Капустін [13], В.І. Кащєєв [14], Д. Ковальов, Т. Сухорукова [15], В. Коржов [16], А. Лукацький [17], В.Н. Носевич [18], Є.А. Олєйніков [25], В.П. Пономарьов [19], Н.В. Пошерстник [20], Г. Раєвський [21], А.І. Соловйов [22], Т.Г. Сухорукова [23], В. Шликов [24], В. Ярочкін [26] та ін.

Розголошення конфіденційної інформації може досить дорого коштувати підприємству. Згідно спільного дослідження ФБР та Інституту комп'ютерної безпеки ("CSI/FBI Computer Crime Security Survey 2005"), в якому взяли участь 700 представників американського бізнесу, середній збиток кожній компанії, яка зареєструвала крадіжку конфіденційних даних в 2005 році, склав 355,5 тис. доларів.

Також за даними PricewaterhouseCoopers и CXO Media (див. "Global State of Information Security 2005"), які опитали більше 13 тис. компаній в 63 країнах світу (в тому числі й Росії та Україні), підраховано, що 33 % та 20 % інцидентів розголошення комерційної таємниці викликані теперішніми та колишніми співробітниками відповідно, 11 % приходиться на частку клієнтів компанії, 8 % відбуваються з вини партнерів, 7 % зумовлені тимчасовими працівниками. Якщо не враховувати клієнтів та партнерів, то за 60 % усіх інцидентів несуть відповідальність колишні, теперішні та тимчасові співробітники компанії, що з урахуванням середньорічного збитку кожній організації (355 тис. доларів), що обумовлює актуальність проблеми розробки політики економічної безпеки підприємства [27].

Постановка завдання. Дослідити систему внутрішнього контролю економічної безпеки підприємства та розробити заходи контролю, які дозволять перевіряти ступінь дотримання економічної безпеки підприємства в частині захисту бухгалтерської інформації, що відповідає поточним завданням та цілям підприємницької діяльності.

Результати. Під контролем економічної безпеки підприємства необхідно розуміти системний процес отримання об'єктивних, якісних та кількісних оцінок про поточний стан економічної безпеки підприємства відповідно до певних критеріїв і показників безпеки. Його основне завдання – об'єктивно оцінити поточний стан економічної безпеки підприємства, а також її адекватність поставленим цілям та завданням бізнесу з метою збільшення ефективності і рентабельності економічної діяльності.

Важливим етапом при забезпеченні надійності бухгалтерської інформації є розробка політики економічної безпеки, яку необхідно впроваджувати на підприємстві. Вона включає правила та норми поведінки при обробці, захисті, а також розповсюдженні конфіденційної облікової інформації. Зокрема, правила визначають, в яких випадках користувач має право працювати з певними даними бухгалтерського обліку. Від надійності комп'ютерної системи залежить суворість та різноманітність правил, які забезпечують політику економічної безпеки.

Політика економічної безпеки включає комплекс принципів, правил, процедур та практичних прийомів щодо захисту конфіденційних даних та інформаційних процесів на підприємстві, а також включає вимоги до управлінського персоналу, працівників технічних служб.

Розробка даної політики залежить від наступних факторів:

– конкретної технології обробки бухгалтерської інформації;

– технічних та програмних засобів обробки бухгалтерської інформації, що використовуються на підприємстві.

Політика економічної безпеки підприємства повинна забезпечити систему заходів захисту бухгалтерської інформації достатньо високого рівня та містити наступні розділи (табл. 1).

Таблиця 1. *Розділи політики економічної безпеки підприємства в частині захисту бухгалтерської інформації*

Назва розділу	*Характеристика розділу*
Терміни і визначення	Основні терміни та визначення, які містяться в політиці економічної безпеки підприємства
Вступ	Необхідність появи даного документа
Мета політики	Цілі створення документу
Сфера застосування	Об'єкти та суб'єкти, які повинні виконувати вимоги даної політики. Політика застосовується до всіх співробітників, що мають будь-яку форму доступу до бухгалтерської інформації в комп'ютерному середовищі підприємства
Політика	Основні рівні захисту щодо забезпечення економічної безпеки підприємства
Відповідальність	Відповідальність за порушення зазначених у попередньому розділі вимог
Історія змін даної політики	Дає можливість відстежити всі зміни, що вносяться до документу

Така структура дозволяє лаконічно охопити всі основні моменти, пов'язані з предметом політики економічної безпеки в частині захисту бухгалтерської інформації. Основними напрями розробки політики економічної безпеки є визначення даних, які необхідно захищати, визначення осіб та якої шкоди вони можуть заподіяти підприємству в інформаційному аспекті, а також виявлення ризиків та визначення схеми їх зменшення до допустимої величини.

Політика встановлює жорсткі вимоги для запобігання незаконному використанню бухгалтерських даних, що є власністю підприємства та його партнерів. В основу системи безпеки бухгалтерської інформації підприємства повинні бути закладені наступні принципи рис. 1.

Всі співробітники підприємства, що мають доступ до бухгалтерської інформації, яка має відношення до третьої сторони та довіреної підприємству в межах ділової співпраці (дані, документація тощо), зобов'язані дотримуватися її конфіденційності.

Положення, що забезпечують захист бухгалтерської інформації, повинні бути внесені до посадових інструкцій співробітників, міститися у відповідних правилах із забезпечення безпеки бухгалтерської інформації та угоді про нерозголошення комерційної таємниці підприємства, яка підписується кожним співробітником при прийнятті його на роботу. Відповідно до цих вимог співробітники підприємства забезпечують конфіденційність бухгалтерської інформації, даних, документація та зобов'язуються здати роботодавцю всі подібні матеріали після закінчення роботи.

Рис. 1. *Принципи безпеки системи бухгалтерської інформації підприємства*

Доповненням політики економічної безпеки є механізм підзвітності, який дозволяє визначати, хто працює в системі та, що робить в певний момент часу. Засоби підзвітності можна розділити на наступні категорії, зображені на рис. 2.

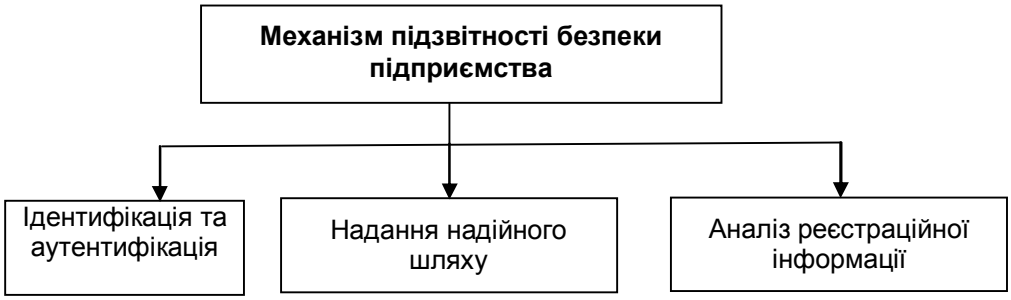

Рис. 2. *Механізм підзвітності безпеки підприємства*

Ідентифікація та аутентифікація полягає в тому, що кожен користувач, перш ніж одержати право на здійснення будь-яких дій в комп'ютерній системі бухгалтерського обліку, повинен ідентифікувати себе. Звичайний спосіб ідентифікації – введення імені користувача при вході в систему. У свою чергу система повинна перевірити аутентичність особи користувача, тобто що саме він є тим, за кого себе видає. Стандартний засіб перевірки аутентифікації – пароль, хоча можуть використовуватися також різного роду особисті картки, біометричні пристрої, такі як, наприклад, сканування сітківки ока або відбитків пальців, або ж їх комбінація.

Надання надійного шляху пов'язує користувача безпосередньо з надійною обчислювальною базою, обійшовши інші, потенційно небезпечні компоненти системи. Мета надання надійного шляху полягає в можливості надати користувачу можливість переконатися в аутентичності обслуговуючої його системи.

Аналіз реєстраційної інформації передбачає наявність засобів вибіркового протоколювання відносно користувачів (здійснюється стеження як за підозрілими особами, так і за подіями, зокрема, вхід та вихід із комп'ютерної інформаційної системи, звернення до видаленої системи, операції з файлами, зміна прав доступу користувачів бухгалтерської інформації).

Протоколювання допомагає стежити за користувачами комп'ютерної системи бухгалтерського обліку та відтворювати здійснені події. Відтворення подій дозволяє проаналізувати випадки порушень, зрозуміти, чому вони стали можливі, оцінити розміри збитку та вжити необхідних заходів щодо уникнення подібних порушень в майбутньому. При здійсненні протоколювання події, що відбулася в комп'ютерній системі бухгалтерського обліку, фіксуються наступні дані (рис. 3).

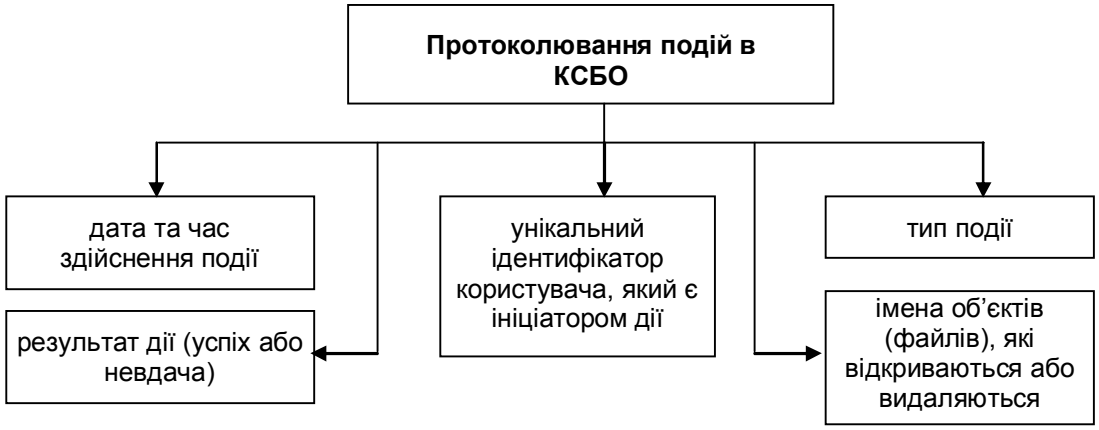

Рис. 3. *Протоколювання події, що відбувалася в комп'ютерній інформаційній системі бухгалтерського обліку*

Додаткові труднощі для забезпечення інформаційної безпеки виникають, якщо підприємство в своїй діяльності використовує комп'ютерні мережі. При розробці системи захисту облікової інформації в комп'ютерному середовищі необхідно пам'ятати, що складна інформаційна система є менш захищеною і розробка її захисту є досить нелегкою справою. Складні системи не завжди можна налагодити належним чином, а різні неточності, які виникають у процесі цього налагодження, можуть призвести до виникнення проблем безпеки.

В сучасних умовах стрімкого використання інформаційних технологій завданням контролю за дотриманням економічної безпеки є перевірка дієвості та ефективності використання систем захисту бухгалтерської інформації на підприємстві.

Для забезпечення економічної безпеки та встановлення контролю за її дотриманням на підприємстві необхідним є створення служби економічної безпеки. В своїй діяльності дана структура повинна:

– керуватися відповідною нормативною базою;

– діяти відповідно до встановлених заходів, тобто виконувати прийняту на підприємстві політику економічної безпеки;

– мати у своєму розпорядженні відповідні засоби, тобто технічне обладнання.

При цьому, даний структурний підрозділ підприємства повинен вирішувати завдання забезпечення безпеки облікової інформації на всіх етапах її накопичення, обробки, використання та зберігання, а також в усіх напрямках господарської діяльності підприємства.

Служба економічної безпеки повинна бути підпорядкована безпосередньо керівнику підприємства, який несе відповідальність за дотримання правил збереження інформації. В деяких випадках керівником даного структурного підрозділу підприємства може бути безпосередньо і сам директор або його заступник.

За участю представників служби економічної безпеки підприємства повинно відбуватись створення корпоративної інформаційної системи підприємства з початку її проектування до моменту введення в експлуатацію. Разом з тим, уже працюючу систему необхідно періодично обстежувати на предмет виявлення нових слабких місць і ризиків, та здійснювати постійний внутрішній контроль над нею. Нехтування щодо безпеки корпоративних систем приводить до великих фінансових втрат у результаті появи та реалізації внутрішніх або зовнішніх загроз.

Висновки. Для будь-якого підприємства при побудові системи безпеки облікових даних необхідним є розробка політики економічної безпеки підприємства, у формі внутрішнього документу, в якій на основі аналізу сучасного рівня та динаміки розвитку інформаційних технологій розглядається систематизоване викладення цілей, завдань та принципів досягнення потрібного рівня економічної безпеки.

Для здійснення внутрішнього контролю за дотриманням економічної безпеки на підприємстві доцільним є створення спеціальної служби, що є підрозділом, призначеним для організації робіт зі створення системи захисту інформації та наступного забезпечення її контролю та функціонування. Проте, створення служби економічної безпеки потребує значних витрат, що може бути не під силу підприємству забезпечувати її функціонування. Тому, забезпечення даних функцій, може покладатися на службу внутрішнього контролю підприємства, бухгалтерську службу або окремого працівника, що працює в складі даних підрозділів або займається супроводом комп'ютерної інформаційної системи підприємства.

ЛІТЕРАТУРА:

1. *Азарова А.О.* Розробка методики визначення економічної безпеки підприємства / А.О. Азарова, О.В. Гаврилова // Економіка: проблеми теорії та практики. Збірник наукових праць. Випуск 191: В 4 т. Том III. – Дніпрпетровськ: ДНУ, 2004. – 318 с.

2. *Александров І.А.* Кластеризація територіальних утворень України за рівнем економічної безпеки / І.А. Александров, О.В. Половян // Економічна кібернетика. – 2000. – № 5-6. – С. 40-47.

3. *Андрощук Г.* Правове регулювання ноу-хау / Г. Андрощук // Інтелектуальна власність. – 2004. – № 10. – С. 29-35.

4. *Андрощук Г.А., Крайнев П.П.* Экономическая безопасность предприятия: защита коммерческой тайны: [монограф.] / Г.А. Андрощук, П.П. Крайнєв. – К.: Издательский Дом "Ин Юре", 2000. – 400 с.

5. *Ареф'єва О.В.* Планування економічної безпеки підприємств / О.В. Ареф'єва, Т.Б. Кузенко. – К: Вид-во Європ. ун-ту, 2004. – 170 с.

6. *Барсуков В.С.* Обеспечение информационной безопасности / В.С. Барсуков. – М., 1996. – 271 с.

7. *Батурин Ю.М.* Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жоздишевский. – М., 1999. – 297 с.

8. *Василевский И.В.* Найти и обезвредить. Техника защиты информации / И.В. Василевский // Система безопасности. – 1995. – № 6. – С. 11-15.

9. *Василец В.И.* Методические основы обеспечения конфиденциальности производственной и коммерческой деятельности акционерного общества / В.И. Василец, В.Н. Голованов // Вопросы защиты информации. – 1994. – № 1. – С. 5-11.

10. *Горячев В.С.* Информация и ее защита / В.С. Горячев // Вопросы защиты информации. – 1994. – № 2. – С. 13-18.

11. *Грэй, Сидней Дж.* Финансовый учет: Глобальный подход: [учеб.-метод. пособие: пер. с англ] / Сидней Дж. Грэй, Белверд Е. Нидлз. – М.: Волтерс Клувер, 2006. – 614 с.

12. *Забродский В.* Теоретические основы оценки экономической безопасности отрасли и фирмы / В. Забродский, Н. Капустин // Бизнес-информ. – 1999. – № 15-16. – С. 35-37.

13. *Капустин Н.* Экономическая безопасность отрасли и фирмы / Н. Капустин // Бизнес-информ. – 1999. – № 11-12. – С. 45-47.

14. *Кащеев В.И.* Обеспечение информационной безопасности коммерческого объекта / В.И. Кащеев // Системы безопасности. – 1995. – № 5. – С. 8-12.

15. *Ковалев Д.* Экономическая безопасность предприятия / Д. Ковалев, Т. Сухорукова // Экономика Украины. – 1998. – № 10. – С. 48-52.

16. *Коржов В.* Сколько стоит безопасность? / В. Коржов // Computerword. – 2004. – № 12: [Електронний ресурс]. – Режим доступу: http://www.outsourcing.ru/content/rus/131/1314-article.asp.

17. *Лукацкий А.* Как связать безопасность компании с ее бизнесом / А. Лукацкий // Корпоративные системы. – 2008. – № 1. – С. 65-72.

18. *Носевич В.Н.* Электронные документы и меры по обеспечению их сохранности (Опыт Республики Беларусь) // Электронный документ и документооборот: Правовые аспекты: Сб. науч. тр. / РАН. ИНИОН. Центр социальных науч.-информ. исслед. Отдел правоведения; РАН. ИГП. Центр публичного права. Сектор информационного права; Отв. ред. – Алферова Е.В., Бачило И.Л. – М., 2003. – 2008 с.

19. *Пономарев В.П.* Оценка уровня экономической безопасности предприятия: материалы Международной науч.-практ. конф. [Настоящее и будущее российской экономики: проблемы, подходы, решения] / В.П. Пономарев. – Пермь: Гос. ун-т, 1999. – С. 189-190.

20. *Пошерстник Н.В.* Бухгалтерский учет на современном предприятии: [учеб.-практ. пособие] / Н.В. Пошерстник. – М.: ТК Велби, изд-во Проспект, 2006. – 552 с.

21. *Раевский Г.* Система экономической безопасности предприятия / Г. Раевский // Частный сыск, охрана, безопасность. – 1994. – № 2. – С. 5-11.

22. *Соловьев А.И.* Экономическая безопасность хозяйствующего субъекта / А.И. Соловьев // Конфидент. – 2002. – № 3. – С. 46-50.

23. *Сухорукова Т.Г.* Концептуальный взгляд на экономическую безопасность предприятия / Т.Г. Сухорукова // Залізничий транспорт України. – 1998. – № 2-3. – С. 9-12.

24. *Шлыков В.В.* Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. – СПб.: “Алетейя”, 1999. – 138 с.

25. Экономическая и национальная безопасность: [учеб.] / Под ред. Е.А. Олейникова. – М.: Экзамен, 2005. – 768 с.

26. *Ярочкин В.И.* Безопасность информационных систем / В.И. Ярочкин. – М. “Ось-89”, 1996. – 197 с.

27. 12 самых громких случаев ИТ-воровства в России: [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/reviews/?2005/12/02/192675.