***Наталія Самородова**, доцент*
Анна Чень
Харківський інститут банківської справи
Університету банківської справи НБУ
м. Харків, Україна

ПРИНЦИПИ ОРГАНІЗАЦІЇ ФІНАНСОВОГО ОБЛІКУ ЯК ОСНОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ

Фінансова інформація є складовою економічної та інформаційної безпеки підприємства . Одним із способів дотримання безпеки є комерційна таємниця, яка обмежує доступ до життєво необхідної інформації. Інформація фінансового характеру, яка оприлюднюється може бути достатньою для будь-якого користувача, а управлінська не підлягає розголошенню. Основним елементом захисту комерційної таємниці від впливу негативних факторів слід вважати належну організацію систему обліку, оскільки масив первинної документації служить підставою для фінансового й управлінського обліку. Організація облікового процесу повинна передбачати схему обробки даних з врахуванням захисту від несанкціонованого їх використання.

Ця проблема знайшла висвітлення у працях таких вчених, як: Клименко В.А., Кириченко О.А., Кім Ю. Г., Дарнопих Г.С., Кашаев А.Н.

Організація передбачає вибір суб'єктів, методики й техніки облікового процесу, що визначається обліковою політикою. Система обліку та її структура залежить від конкретного суб'єкта господарювання відповідно до потреб його керівництва з урахуванням вимог законодавства щодо отримання якісної інформації для зовнішніх та внутрішніх користувачів із дотриманням вимог економічної безпеки підприємства. Основні принципи організації фінансового обліку та фінансової звітності наведені в Законі України « Про бухгалтерський облік та фінансову звітність в Україні» [1,], а саме: обачність, повне висвітлення, автономність, послідовність, безперервність, нарахування та відповідність доходів і витрат, превалювання сутності над формою, історична (фактична) собівартість, єдиний грошовий вимірник, періодичність.

Кириченко О. А. та Кім Ю. Г. [2, с. 56] підкреслюють, що організацію обліку слід здійснювати із застосуванням певних принципів, що забезпечать злагодженість, ефективність та економічну безпеку роботи підприємства, а тому до складу принципів слід додати:

- принцип комплексності, згідно з яким при розробці системи захисту облікових даних необхідно передбачати різні види можливих загроз для безпеки підприємства, включаючи канали несанкціонованого дос-

тупу до бухгалтерської інформації та можливі для нього засоби захисту;

- принцип безпеки та контролю даних, який передбачає захист цінної облікової інформації, шляхом встановлення обмеження користувачів, віднесення її до інформації конфіденційного характеру та запровадження обмежень при роботі з нею;

Застосування цих засобів потрібно порівнювати з можливими видами загроз, а засоби захисту облікової інформації повинні функціонувати в межах єдиного комплексу захисту конфіденційної інформації підприємства взаємно доповнюючи один одного у функціональному і технічному аспектах.

Захист облікових даних, що складають комерційну таємницю, слід покладати не лише на службу безпеки, й на управлінський персонал підприємства – від керівника, до технічного персоналу. Кваліфікація та кількість працівників, які забезпечують безпеку господарюючого суб'єкта, повинні відповідати завданням економічної служби безпеки, щоб не бути «тягарем» для бюджету підприємства, або загрозою для діючого керівництва. На жаль, із стрімким розвитком інформаційно-технічного забезпечення не всі працівники мають належний рівень компетенції при користуванні інформаційними системами, що призводить до значних втрат на підприємстві. Так, наприклад, якщо комерційна організація допускає витік більше 20% важливої внутрішньої інформації, то вона в 60 випадках з 100 банкрутує [3, с. 62], а також, 93% компаній, що залишилися без доступу до власної інформації на термін понад 10 днів, залишили бізнес, причому половина з них заявила про свою неспроможність негайно [3, с. 63]. Є дані про те, що 76% витоку інформації становлять не навмисні дії персоналу, а безвідповідальність та некомпетентність співробітників підприємства [4, с. 192].

До некомпетентних дій персоналу Клименко О.А. [3, с.62] та Дарнопих Г. С. [5, с.143] відносять:

- відкриття на своєму комп'ютері файлів, надісланих електронною поштою або програмами миттєвого обміну повідомленнями, які одержані від невідомих адресатів;
- встановлення неліцензійного програмного забезпечення, не потрібного для виконання функціональних обов'язків працівника;
- використання паролів «за замовчуванням», створення простих паролів, або небажання змінювати паролі протягом тривалого часу , «запам'ятовування» пароля у вікнах уведення, особливо на комп'ютерах для публічного доступу;
- робота з конфіденційними документами в місцях публічного доступу;
- недотримання правил супроводження всіх відвідувачів, що приходять до вас на роботу;

- повідомлення по телефону будь-яких даних про обліковий запис, логіни, паролі;
- нецільове використання мережевих ресурсів, тощо.
- Для усунення некомпетентних дій працівників вказані автори пропонують використання таких методів боротьби з втратою облікової інформації:
- використання міжнародних стандартів стосовно гарантування інформаційної безпеки;
- підвищення кваліфікації персоналу в галузі економічної безпеки ;
- контроль за виконанням вимог політики, інструкцій та правил стосовно гарантування інформаційної безпеки;
- проведення зовнішнього та внутрішнього аудиту;

Вважаємо, що реалізація таких захисних механізмів через можлива резервування інформації, забезпечення її доступності, цілісності та конфіденційності, шляхом блокування некомпетентних дій працівників.

Таким чином, на формування економічної безпеки підприємства впливає не лише організація системи обліку, а й компетенція працівників у даній галузі. Організацію економічної безпеки слід базувати на ефективній системі заходів із необхідним правовим, економічним, організаційним та інформаційним обгрунтуванням, що передбачає формування оптимальної структури інформаційної служби та служби безпеки.

Головним пріоритетом захисту інформації на підприємстві є розробка заходів спрямованих на збереження інформаційних ресурсів, що міститься в інформаційній базі підприємства які є об'єктом зацікавленості конкурентів. Необхідним атрибутом захисту облікової інформації є кадрова робота з персоналом підприємства.

Література:

7. Закон України « Про бухгалтерський облік та фінансову звітність в Україні» №996-XIV від 16.07.1999 р.: [Електронний ресурс].- Режим доступу: www.zakon.rada.gov.ua.
8. Кириченко О.А., Кім Ю.Г. Методологічні основи економічної безпеки суб'єктів господарювання в трансформаційній економіці // Актуальні проблеми економіки.- 2008.- №12.- С. 53-65.
9. Клименко В. Внутрішні загрози інформаційній безпеці організації // Вісник НБУ.- 2008.-№5.- С. 62-63.
10. Кашаев А. Н. Организация бухгалтерского учета в производственных обьединениях // Финансы и статистика.- 2007.- №4.- С. 192.
11. Дарнопих Г. Сучасні проблеми економічної безпеки України // Вісник Академії правових наук України.- 2009.- №1.- С. 142-150.