ПОПКО Н.В.
ст. гр. ОАБм-11

ПОЛІТИКА ЕКОНОМІЧНОЇ БЕЗПЕКИ В ЧАСТИНІ ЗАХИСТУ БУХГАЛТЕРСЬКОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

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.

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.

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.

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. 1.

Рис. 1. 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. 2.).

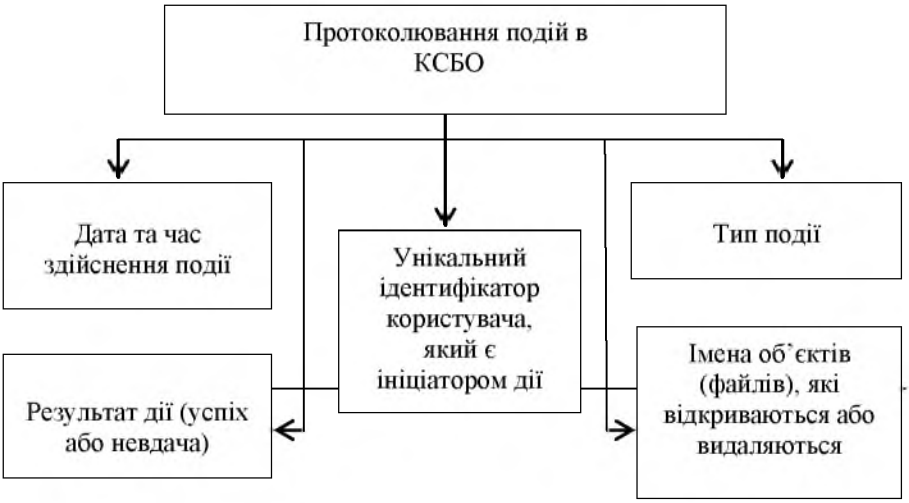

Рис. 2. Протоколювання події, що відбувалася в комп'ютерній інформаційній системі бухгалтерського обліку

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 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.

Література:

1. Адамик О.В. Бухгалтерський облік як основа інформаційного забезпечення оподаткування підприємства // Галицький економічний вісник. – 2004. – № Випуск 1. – С. 109-114.

2. Адамик, О. В. Бази і сховища даних – інформаційний фундамент бухгалтерського обліку та аналізу // Економічні, управлінські, правові та інформаційно-технічні проблеми діяльності підприємств: колективна монографія/ за заг. ред. Л. М. Савчук, М. Фіц.–Дніпро: Герда, 2016.–528 с. ISBN 978-617-7097-58-6. – С. 330-341

3. Артеменко Л.П., Бебешко Д.В. Стратегічні напрямки забезпечення економічної безпеки підприємства // Проблеми системного підходу в економіці. - № 2. – 2009: [Електронний ресурс]. – Режим доступу: URL http://www.nbuv.gov.ua/e-journals/PSPE/2009_2/Artemenko_209.htm

4. Шигун М.М. Принципи внутрішнього контролю в системі економічної безпеки підприємства / М.М. Шигун // Науковий вісник Ужгородського університету. – 2014. – Розділ 4. Бух- галтерський облік та аудит. – С. 159–162.