Рожелюк В.М., д.е.н., доц.,
Денчук П.Н., к.е.н., доц.
Тернопільський національний економічний університет

ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОБЛІКОВОЇ ІНФОРМАЦІЇ

Виступаючи генератором інформації, система бухгалтерського обліку потребує надійного захисту, оскільки, вочевидь, підпадає під значні ризики. У теорії ризиків поширений їх поділ на політичні, економічні, банківські, фінансові, кредитні, комерційні тощо.

Принципове значення для даного дослідження має класифікація ризиків та загроз за природою походження на зовнішні та внутрішні. Вона дає змогу відокремити об'єктивні загрози від суб'єктивних, тобто нав'язані нам і створені нами ж самими.

До зовнішніх загроз безпеці бухгалтерської інформації можна віднести розвідувальну діяльність конкурентів, несанкціонований доступ до закритої інформації та інформаційних ресурсів, промислове шпигунство, фінансова розвідка, прослуховування, злом комп'ютерної мережі тощо.

Будь-які методи захисту інформації мають відповідати вимогам, що є несумісними: високий ступінь захисту інформації та зручність у використанні. Ідеальним є той варіант, коли робота всіх механізмів захисту є непомітною для користувача інформаційної системи та проявляється лише при спробі користувача вийти за межі своїх функціональних повноважень. Проте на практиці це поки що не реалізовано та використовуються різні компромісні варіанти. В залежності від ступеня секретності інформації нами виділено наступні групи загроз безпеці облікової інформації:

1) група технічних загроз сформована під впливом комп'ютеризації обліку. Коли облік в переважній більшості вівся вручну технічними загрозами можна було вважати фізичне знищення документів через пожежу, підтоплення тощо. Сьогодні до цієї групи перш за все віднесено всі можливі неполадки технічного та програмного забезпечення, які можуть призвести до втрати інформації. Організаційні заходи із захисту інформації в комп'ютеризованих системах мають охоплювати етапи проектування, розробки, виготовлення, випробовування, підготовки до експлуатації та експлуатації системи. Витік інформації про важливі характеристики системи може призвести до зниження безпечності інформаційного обміну через можливість використання зловмисником слабких місць в реалізації системи або певних конструкційних особливостей апаратури (наприклад, організація додаткових каналів розповсюдження інформації через підключення до легальних інформаційних каналів). Для мінімізації даної групи загроз потрібно періодично формувати архів інформації, створювати резервні копії, вживати заходи антивірусної безпеки.

2) група загроз отримання неправдивої інформації включає в себе можливість генерування інформації, яка суперечить дійсності. Такі загрози можуть бути спричинені ненавмисним перекрученням даних шляхом допущення арифметичних помилок, недостатньою компетенцією бухгалтера, отриманням неточних вхідних даних тощо. До даної групи загроз належить також і навмисне перекручення

інформації бухгалтером (фальсифікація), яке може бути спричинене власними інтересами бухгалтера (наприклад, стосовно незаконного привласнення коштів). Для зменшення можливості виникнення даних загроз важливо мати бухгалтера з високим рівнем компетенції та професіоналізму, а також постійно вживати заходів щодо підтримання даного рівня. Крім того, на підприємстві має бути побудована дієва система контролю за функціонуванням системи обліку.

3) група, пов'язана з необхідністю забезпечення конфіденційності інформації – загрози розголошення, яка, в свою чергу, поділяється залежно від джерела можливого витоку інформації від внутрішніх та зовнішніх її користувачів.

4) група, що включає всі загрози спричинені недосконалою організацією системи комунікації на підприємстві, а також недоліки управління в даній сфері, які не увійшли до попередніх груп. До них можна віднести недотримання встановленого регламенту збирання, оброблення, зберігання та передачі бухгалтерської інформації, недостатнє фінансування заходів інформаційної безпеки тощо. Рішенням даних загроз є усвідомлення керівниками важливості внутрішньої інформаційної безпеки та прийняття заходів щодо їх усунення (мінімізації).

Тому вважаємо за доцільне запропонувати наступні заходи, які сприятимуть їх мінімізації: для зменшення ймовірності виникнення технічних загроз варто приділяти належну увагу періодичній архівації інформації, створенню резервних копій, вжиттю заходів антивірусної безпеки; для мінімізації загрози генерування недостовірної інформації варто створити на підприємстві надійну систему контролю за функціонуванням облікової системи, а також підтримувати рівень професіоналізму та компетенції бухгалтера; для убезпечення підприємства від витоку інформації варто організувати систему комунікації, яка надавала б інформацію внутрішнім користувачам виключно в межах їх професійних потреб, забезпечити відповідні умови праці бухгалтеру та визначити його відповідальність; а також приділяти належну увагу фінансуванню заходів інформаційної безпеки тощо.