УДК 657

В.М. Рожелюк
к.е.н., доцент
Тернопільський національний економічний університет

ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОБЛІКОВОЇ ІНФОРМАЦІЇ

Постановка пороблеми. *У сучасних умовах роль інформації важко переоцінити.* Навколо інформаційних джерел, одним з яких є бухгалтерський облік, точаться справжні війни. Так, Л. Стрельбицька та М. Стрельбицький [3, с. 6] стверджують, що сьогодні на нашій планеті триває Четверта світова війна. Її формальним початком вважається виступ колишнього прем'єра Великої Британії В. Черчілля (1946 р.), коли він оголосив "хрестовий похід" *союзу англомовних націй проти* Радянського Союзу. Інформаційна війна ведеться упродовж останніх десятиліть і в Україні. При чому, якщо інформаційним революціям і світовим війнам ведеться відлік, то інформаційних війн – безліч, як локальних, так і масштабних. Інформаційні війни можуть вестись за технології, розробки, а також війни за інформацію, яка генерується в системі бухгалтерського обліку. Таким чином, постає питання забезпечення надійної системи захисту, конфіденційності бухгалтерської інформації, організації внутрішньої системи комунікації.

На актуальність проблеми вказують і статистичні дані. Так, організація CERT, опитавши більше 800 компаній, встановила, що кожна друга компанія хоча б раз протягом року постраждала від витоку інформації. При цьому за даними спільного дослідженням ФБР і Інституту комп'ютерної безпеки, в якому взяли участь 700 представників американського бізнесу, середній збиток кожній компанії, яка зареєструвала крадіжку конфіденційних даних у 2005 році, склав 355,5 тис. доларів [1].

Аналіз останніх досліджень і публікацій. Питання захисту облікової інформації знайшли своє відображення в наукових працях українських і російських вчених І.А. Белоусової, О.М. Брадула, Ф.Ф. Бутинця, Б.І. Валуєва, В.В. Гніліцький, В.В. Євдокимова, В.Б. Івашкевича, М.Д. Корінька, М.Ф. Кропивка, С.З. Мошенського, О.В. Олійник, Є.Г. Орєхов, В.Ф. Палія, Л.В. Чижевської, а також таких науковців як К.П. Боримська, Л.В. Гнилицька, А.П. Дикий, О.О. Мозгова, Н.В. Наконечна, В.Ю. Світлична, Л.С. Сорока, та ін. Проте, з кожним днем кількість варіантів інформаційного шахрайства нестримно зростає, що зумовлює необхідність подальшого моніторингу існуючих проблем.

Метою дослідження є пошук можливих заходів мінімізації загроз облікової інформації.

Викладення основного матеріалу дослідження. 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. Коли ж йдеться про інформаційні, то тут, як правило, оперують поняттям загрози, класифікація яких наведена на рис. 1.

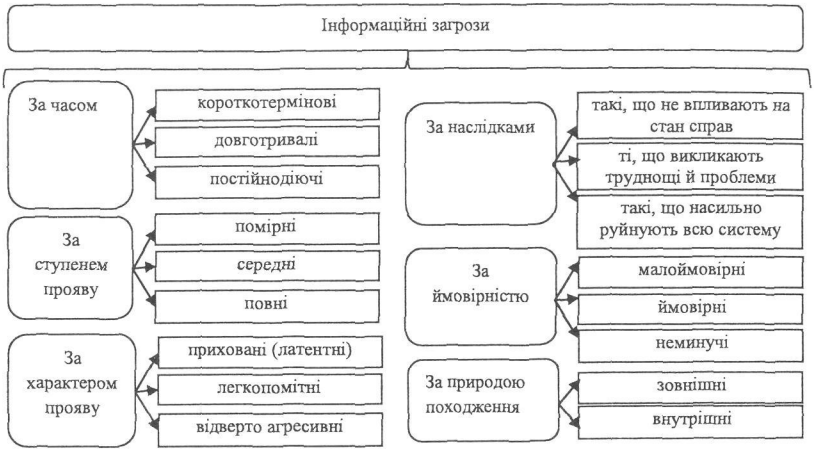

Рис. 1. *Класифікація інформаційних ризиків та загроз (розроблено на основі [3, с. 7])*

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.

Проте, як зазначають Л. Стрельбіцьціка, М. Стрельбіцький, переважна більшість загроз в інформаційній сфері (приблизно 80 %) мають внутрішній, суб'єктивний характер. Вони значною мірою виходять від самого підприємства і воно повинне їх скеровувати та усувати. Це залежить лише саме від підприємства, його волі, готовності і професійної зрілості [3, с. 7].

За словами М.К. Ніколаємої [2, С. 96], в середньому 17 % всіх загроз інформаційної безпеки виходить ззовні, 1 % – загрози з боку випадкових осіб і 82 % – загрози внутрішні, тобто від персоналу фірми (рис. 2).

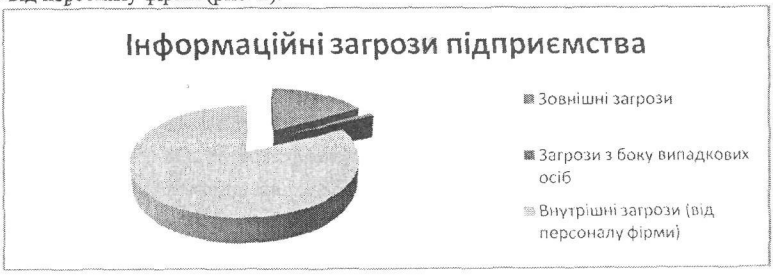

Рис. 2. *Джерела інформаційних загроз підприємства (розроблено за даними [2, С. 96])*

До того ж, за відомостями PricewaterhouseCoopers і CXO Media, що опитали більше 13 тис. компаній в 63 країнах світу (в тому числі і Росії), більше половини (60%) всіх інцидентів IT-безпеки за минулий рік були викликані саме інсайдерами. Аналітики підрахували, що 33 % та 20 % інцидентів викликані нинішніми та колишніми співробітниками відповідно, 11 % припадають на частку клієнтів компанії, 8 % відбуваються з вини партнерів і, нарешті, 7 % викликані тимчасовими службовцями (контрактниками, консультантами і т.д.). Навіть якщо не враховувати клієнтів і партнерів, то за 60 % всіх інцидентів несуть відповідальність нинішні, колишні та тимчасові співробітники компанії, що з урахуванням середнього щорічного збитку кожній організації в 355 тис. доларів піднімає проблему внутрішньої інформаційної безпеки на перше місце в списку пріоритетів керівництва компанії [1].

На основі проведеного дослідження серед внутрішніх загроз облікової інформації виділено чотири основні групи та запропоновано заходи їх мінімізації, зазначені на рис. 3.

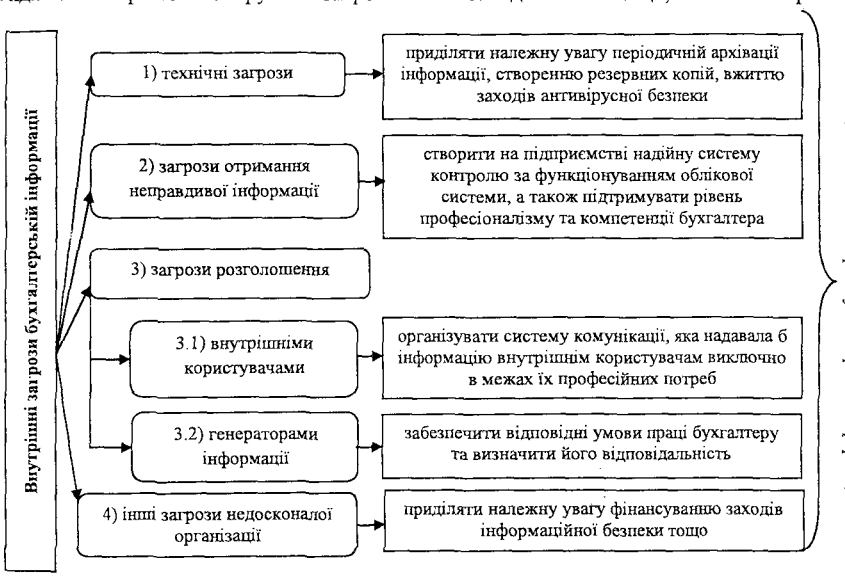

Рис. 3. *Внутрішні загрози бухгалтерській інформації та заходи їх мінімізації (власна розробка)*

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 нереалізовано та використовуються різні компромісні варіанти. В залежності від ступеня секретності інформації: або зручність

використання інформаційної системи, або більший ступінь захисту інформації. Розглянемо детальніше кожну з виділених на рис. груп загроз.

1) Сутність групи 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 архівувати інформацію, створювати резервні копії, вживати заходи антивірусної безпеки.

2) Загрози отримання неправдивої інформації включають 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) Наступною важливою групою загроз є група, пов'язана з необхідністю забезпечення конфіденційності інформації – група загрози розголошення, яка, в свою чергу, поділяється залежно від джерела можливого витоку інформації.

3.1) Одним з можливих джерел витоку інформації є внутрішні її користувачі. Усталена теорія щодо того, що зовнішнім користувачам надається обмежена кількість інформації, а внутрішнім повна, є недосконалою. Адже на кожному конкретному підприємстві необхідно чітко класифікувати внутрішніх користувачів і визначити, яку саме інформацію їм необхідно надавати. При чому класифікувати не лише на працівників та управлінців, а з високим рівнем деталізації – менеджеру якого рівня, якого підрозділу, яку частку інформації необхідно отримати для виконання своїх функцій. Необхідність такої системи спричинена можливою плинністю кадрів, переманюванням працівників, їх підкупом, промисловим шпигуванням. Організація такої системи конфіденційності облікової інформації дасть змогу мінімізувати можливий її витік.

Серед не управлінського персоналу також має бути організована відповідна система комунікацій. Наприклад, суми розміру заробітних плат працівників доцільно тримати в

таємниці з метою уникнення додаткових конфліктів. Для цього при виплаті заробітної плати варто оформлювати ВКО, адже використання платіжних та розрахунково-платіжних відомостей дає змогу працівникам ознайомитись зі ставками колег.

Крім того, варто підписувати з працівниками інсайдерські договори про нерозголошення інформації. Такий інструмент спрацьовує скоріше на психологічному рівні, ніж на правовому, проте є дієвим.

Таким чином, основними організаційними заходами захисту інформації від витоку через користувачів можуть бути:

1. створення відповідних режимів роботи з інформаційною системою з урахуванням ступеня секретності інформації;

2. створення та впровадження інструкцій та положень по забезпеченню режимів секретності;

3. створення захищених зон інформаційної системи з обмеженим доступом та організацією служби безпеки;

4. розмежування кола задач за певними виконавцями та обмеження доступу до інформації в цілому;

5. постійний контроль за виконанням режимів секретності та облік доступу до інформації відповідно до кожного оператора;

6. встановлення та розподілення відповідальності за витік інформації за службами безпеки та конкретними особами;

7. підписання інсайдерських договорів.

3.2) Іншим джерелом є самі працівники бухгалтерії, які, маючи таку «зброю» в своїх руках, можуть стати основним джерелом загрози для інформаційної безпеки підприємства. Виділимо інструменти, які може використовувати підприємство для забезпечення збереженості інформаці.

Першим з них є визначення відповідальності бухгалтера за порушення, що стосуються надання не достовірної інформації, а також розголошення конфіденційності інформації. Даний інструмент має впроваджуватись як на макрорівні, шляхом передбачення різних видів відповідальності (від адміністративної до кримінальної) за вказані дії в нормативних актах, так і на мікрорівні, шляхом окреслення норм відповідальності бухгалтера в посадових інструкціях та інших внутрішніх розпорядчих документах підприємства.

Іншим дієвим інструментом є створення бухгалтеру відповідних умов. Достойна заробітна плата, гарні умови праці, визнання в колективі, ідейна прив'язаність, додаткові стимули в результатах діяльності сприятимуть збільшенню вірогідності відмови у разі переманювання бухгалтера до конкурента чи пропозиції надати інформацію.

Ще одним інструментом можна вважати Кодекс етики професійних бухгалтерів, затверджений Міжнародною федерацією бухгалтерів, який використовується і в Україні. Одним з наведених в ньому принципів є принцип конфіденційності, який передбачає не розголошення третім особам одержаної в процесі надання професійних послуг (окрім випадків, коли є юридичне чи професійне право або обов'язок розкривати цю

інформацію), а також не використання її у власних цілях. Аудиторською палатою України він прийнятий до обов'язкового виконання. В системі бухгалтерського обліку України він є лише рекомендованим, хоча цілком доцільно було б зробити його обов'язковим.

4) Останньою групою інформаційних загроз є 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).

Запропоновані заходи безпеки інформації доцільно запроваджувати через положення про облікову політику, а також посадові інструкції, графіки документообігу, контракти, договори, угоди з працівниками, накази керівника та інші документи, що регламентують внутрішній розпорядок.

Висновки та пропозиції. На підставі проведеного дослідження виявлено необхідність організації надійного захисту облікової інформації. Шляхом окреслення найпоширеніших інформаційних загроз встановлено, що особливої уваги потребують загрози внутрішнього характеру. 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.

Список використаних джерел

1. 12 самых громких случаев ИТ-воровства в России / CNews: [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/reviews/?2005/12/02/192675.

2. Николаева М.К. вопросы аутентификации электронного документооборота в информационных инфраструктурах в торгово-экономической деятельности / М.К. Николаева // Вестник Российского государственного торгово-экономического университета. – 2007. – № 4 (20).

3. Стрельбицька Л. Інформаційна безпека у сфері державного управління / Л. Стрельбицька, М. Стрельбицький // Юридичний вісник України. – 2010. – № 37(793). – С. 12.