Сауліна А.І. – слухачка магістратури юридичного факультету;
Рибальченко Л.В. – науковий керівник, доцент кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ).

ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Сучасний етап соціально-економічного розвитку характеризується значними політичними, економічними, соціальними та екологічними змінами, стрімким розвитком науково-технічного прогресу, що проникає у всі сфери життєдіяльності людини. Кризові явища, що наростають в державі, посилюють невизначеність економічного становища та вимагають від суб'єктів господарювання посилення уваги до питань власної економічної безпеки, виявлення та нейтралізації можливих загроз, небезпек та ризиків, здатних негативним чином вплинути на стан та результати їх діяльності.

Економічна безпека підприємства – це запобігання усіляких загроз діяльності господарюючого суб'єкта, ефективне використання ресурсів для того, щоб забезпечити стале функціонування комерційної структури. Правильно побудована система забезпечення економічної безпеки дозволить проводити постійний моніторинг за діяльністю організації з метою виявлення загроз і профілактики в діяльності конкурентів, а також дозволить побудувати ефективну методику боротьби з виникаючими проблемами. Загрози діляться на внутрішні і зовнішні. До внутрішніх загроз можна віднести витік інформації, всілякі дії працівників організації, які можуть нашкодити діяльності організації, проблеми з партнерами фірми і так далі. До зовнішніх загроз відноситься недобросовісна конкуренція на ринку товарів і послуг, правопорушення законодавства з боку посадових осіб, а також постійна зміна законодавства. Для того, щоб правильно оцінити можливість виникнення такого роду загроз, необхідно проводити профілактичну роботу і боротьбу з подібними проблемами з метою побудови ефективної системи забезпечення економічної безпеки комерційної структури.

Важливими завдання економічної безпеки підприємства виступає: оцінка ризиків підприємства та їх аналіз; уникнення можливих ризиків та прогноз стану захисту підприємства; захист конфіденційності інформації та комерційної таємниці; ефективне та стратегічне управління системою економічної безпеки підприємства. До останньої належить: захист комерційної таємниці та конфіденційної інформації, інформаційна безпека, внутрішня та зовнішня безпека, конкурентна розвідка, кадрова, виробнича, фінансова, податкова та силова безпеки, а також інші.

Корпоративне шахрайство – одна з актуальних проблем сучасності. За статистикою, 5% прибутку світові компанії втрачають щорічно через несум-

лінні дії своїх співробітників. В Україні цей показник ще більший – у різних випадках він досягає 10–15 %. Ідеться тільки про ті втрати, які оприлюднені компаніями [1]. Ключовими ризиками, які провокують шахрайство у 2019 році є: відсутність систем внутрішніх контролів; самоусунення власника від прямого управління компанією; відсутність критеріїв виміру ефективності бізнесу; особисте небажання власника впроваджувати заходи протидії шахрайству; акцент на готівку при проведенні фінансових транзакцій.

Найкрупнішою у світі організацією по боротьбі із шахрайством ACFE досліджено, що у 2018 році у Східній Європі, а також Західній і Центральній Азії із 86 випадків найбільшим з професійних шахрайств є незаконне присвоєння активів, частка якого становить 83% від загальної частки усіх порушень. Ці випадки спричинили втрату у розмірі 150 000 доларів США. Фінансові схеми шахрайства були найменш поширеними і становили 10% від усіх випадків, а корупційні схеми траплялися у 60% випадків та спричинили у середньому втрату 300 000 доларів США. До організацій, які є жертвами професійного шахрайства належать: приватні компанії – 50% (збитки 115 тис.дол.США), публічні компанії – 43% (збитки 155 тис.дол.США), урядові – 1; неприбуткові – 2%, інші – 3% [2]. Із 86 випадків професійного шахрайства у Східній Європі, а також Західній і Центральній Азії у 2018 році в Україні лише 3, що менше, ніж середнє значення 4,3 з усіх випадків. Найбільше випадків професійного шахрайства у Сербії (9), Румунії (11), Турції (13) та Росії (15).

Цікавим фактом є те, як розмір організації пов'язаний із ризиком професійного шахрайства. З рис. 1 видно, що найбільший відсоток таких випадків у Східній Європі, а також Західній і Центральній Азії належить підприємствам, в яких кількість працівників становить від 100 до 999 (32%). Ці організації зазнали найбільших втрат на 1 млн.дол.США. Організації з кількістю від 1000 до 9999 працівників становлять 31% випадків, мали середню втрату у розмірі 30 тис. доларів США. Великі організації, де понад 10 000 працівників, складали 26% від усіх випадків понесли в середньому втрату в розмірі 275 тис.дол.США.

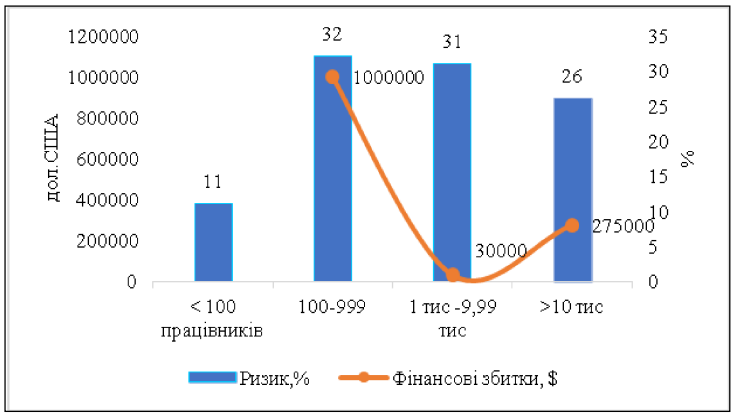

Рис. 1. Залежність розміру збитків від кількості працівників в компанії

Таким чином, для підприємств професійне шахрайство завдає значні збитки. Тому необхідно або залучати консультантів з боку, або збільшувати підрозділ, який займається забезпеченням економічної безпеки всієї організації в цілому. На підприємстві користуються певним набором математичних методів аналізу підприємства. У той же час, необхідно використовувати неструктуровані методи аналізу, що ускладнює отримати кількісні оцінки рівня забезпечення економічної безпеки. Сюди можна віднести: випуск продукції, рівень заробітної плати працівників, витрати на маркетингові заходи, щодо реалізації продукції на ринку товарів і послуг тощо.

Використані джерела:

1. Артем Ковбель. Шахрайство в компанії: що потрібно знати бізнесу. [Електронний ресурс]. – Режим доступу: https://uteka.ua/ua/publication/commerce-12-pravovie-soveti-67-moshennichestvo-v-kompanii-chto-nuzhno-znat-biznesu
2. Report To The Nations. 2018 Global Study On Occupational Fraud And Abuse. [Електронний ресурс]. – Режим доступу: https://www.acfe.com/report-to-the-nations/2018/#download

Свиридова М.С. - курсант 4 курсу факультету підготовки фахівців для підрозділів кримінальної поліції;
Прокопов С.О. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Актуальним питанням на сьогоднішній день постала гібридна агресія до нашої країни з боку Росії. Постійно, зарубіжні країні планують ввести новітні зміні в інформаційний простір та намагаються вдосконалити технології його захисту.

Увага до цього питання дуже довго не була загострена з боку влади нашої держави, аж поки в червні 2017 року не сталась кібератака. Ця кібератака, повністю на певний період часу заблокувала діяльність не тільки тисячі компаній, але й нормальну діяльність державних органів[2]. Вірус, яким були заражені персональній комп'ютери, вимагав викуп у розмірі певної суми (валюта-доллар). Саме цією подією, весь світ зрозумів наскільки важлива кібербезпека та наскільки вона в нас не розвинена. Тому, з боку законодавства було прийнято новий закон, яким має напрям діяльності – сформувати загальнодержавну кібезбезпеку. На основі цього було створено відповідні підрозді-