УДК 347.711 : 65.012.8

Лічман Т. В.
Університет економіки та права «КРОК»

КЛАСИФІКАЦІЯ ТА АНАЛІЗ ЗАГРОЗ БЕЗПЕЦІ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ПІДПРИЄМСТВА

Досліджено категорію «загрози» безпеці комерційної таємниці підприємства як фактору, що визначає механізм організації захисту комерційної таємниці в системі економічної безпеки підприємства.
Ключові слова: комерційна таємниця, загрози, економічна безпека підприємства.

Постановка проблеми. Діяльність з організації системи економічної безпеки підприємства полягає у виявленні факторів, явищ або процесів, що можуть завдати шкоду підприємству або негативно вплинути на його функціонування. Такі фактори, явища або процеси є загрозами, а система економічної безпеки підприємства має бути організована таким чином, щоб завчасно попереджати загрози або максимально локалізувати їх негативний вплив. Інформаційна безпека є функціональною складовою економічної безпеки, а тому своєчасне виявлення загроз комерційній таємниці й реагування на них мають першочергову важливість у практичній діяльності по захисту життєво важливих інтересів підприємства. Характер і рівень загроз безпеці визначають основні напрями діяльності щодо їх попередження і локалізації, форми, способи, засоби і методи вирішення завдань забезпечення безпеки при раціональному використанні наявних обмежених ресурсів підприємства.

Аналіз останніх досліджень і публікацій. Питання організації системи економічної безпеки підприємства є предметом наукових досліджень як вітчизняних, так і закордонних вчених (О. А. Кириченко, С. М. Лаптєв, О. І. Захаров, П. Я. Пригунов [1], Л. В. Гнилицька [2], О. Ю. Захаров [3] та інші). Проблемам захисту інформаційних ресурсів підприємства, зокрема комерційної таємниці, присвячували свої публікації В. С. Сідак [4], І. Б. Ткачук [5], В. І. Ярочкін [6], В. П. Бабак [7], Г. О. Андрощук, П. П. Крайнєв [8], Д. Р. Пескова [9] та інші.

Не вирішені раніше частини загальної проблеми. Питанням загроз безпеці комерційної таємниці підприємства в системі його економічної безпеки не присвячено спеціальних наукових досліджень та публікацій, а їх аналіз здійснюється переважно в рамках аналізу загроз економічній безпеці підприємства взагалі. При цьому, загрози безпеці комерційної таємниці підприємства, володіючи загальними рисами, притаманними загрозам безпеці взагалі, все ж таки мають свою специфіку, обумовлену об'єктом захисту.

Метою статті є виокремити та дослідити загрози безпеці комерційної таємниці підприємства, провести їх класифікацію за різними критеріями, а також проаналізувати окремі види загроз.

Виклад основного матеріалу дослідження. В умовах існуючої конкуренції між суб'єктами господарської діяльності інформація стає цінним об'єктом, оскільки володіння інформацією в ринковій економіці необхідне для ведення конкурентоспроможної господарської діяльності. У зв'язку із цим комерційна таємниця та її захист у системі економічної безпеки підприємства набувають пріоритетного значення.

У науковій літературі описані різні шляхи організації системи економічної безпеки підприємства. При цьому, більшість вітчизняних та закордонних авторів, з якими ми погоджуємося [1; 2; 6], при побудові системи економічної безпеки підприємств включають до неї три взаємопов'язані елементи (категорії): «інтереси – загрози – захист», які є основою механізму цього процесу (рис. 1).

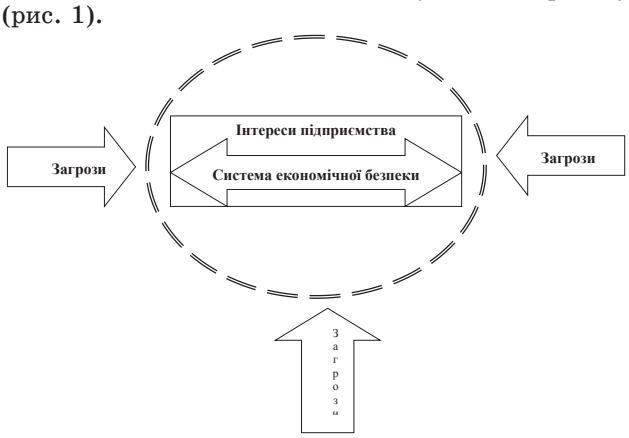

Рис 1. Механізм формування системи економічної безпеки підприємства

Джерело: складено автором

Отже, ключове значення в організації системи економічної безпеки підприємства відіграють загрози.

Одні вчені під загрозою розуміють конкретну і безпосередню форму небезпеки або сукупність негативних чинників чи умов [10, с. 21]. Інша точка зору полягає в розумінні під загрозою сукупності умов, процесів, чинників, які перешкоджають реалізації економічних інтересів суб'єктів господарської діяльності чи створюють небезпеку для них [11, с. 215].

Важко не погодитися із українським ученим А. Марущаком, який зазначає, що за умов невизначеності існує суперечність між теоретично досконалим і практично можливим підходами. Теоретично досконалий підхід полягає в тому, щоб урахувати всі можливі варіанти сценаріїв. Однак практично це здебільшого неможливо зробити, бо доведеться враховувати надто багато альтернатив [12].

Вітчизняні дослідники визначили поняття «загрози економічній безпеці підприємства» як наявність таких потенційних або реальних умов, факторів чи дій фізичних та юридичних осіб, що порушують нормальний фінансово-економічний стан суб'єкта підприємницької діяльності і здатні заподіяти великої шкоди аж до припинення його діяльності [1, с. 189].

Виходячи із викладеного, під загрозами безпеці комерційної таємниці підприємства можна розуміти окремі явища, події, процеси, настання (плинність, побічний результат) яких може впли-

нути на захищеність комерційної таємниці підприємства та привести до негативних наслідків (прямих збитків, неодержаного прибутку, підриву іміджу, зміни в планах, часових втрат тощо).

Комерційна таємниця постійно піддається різним загрозам. Заходи щодо забезпечення безпеки підприємства повинні бути спрямовані на виключення фактів втрати (розголошення, витоку) конфіденційної інформації та недопущення несанкціонованого доступу до неї. Реалізація цих заходів має забезпечувати не тільки власне безпеку комерційної таємниці, а й сприяти стабільному (сталому) розвитку підприємства, збільшенню його доходів або досягнення іншої мети.

Загрози комерційній таємниці підприємства можуть бути дуже різноманітними, а їх класифікація багатогранною. У даному дослідженні класифікація загроз комерційній таємниці проведена за різними ознаками та критеріями, що схематично зображено в табл. 1.

Таблиця 1

Класифікація загроз комерційній таємниці підприємства

Критерії	Різновиди
За джерелом загрози	Зовнішні (промислове шпигунство, незаконні дії конкурентів, крадіжка матеріальних цінностей); внутрішні (розголошення працівниками конфіденційної інформації, низька мотивація персоналу, низька ефективність діяльності служби безпеки)
За ступенем тяжкості наслідків	Загрози з високою тяжкістю наслідків призводять до різкого погіршення всіх фінансово-економічних показників і припинення діяльності фірми; середньої – подолання наслідків вимагає більших витрат, але не вимагає тривалого часу; низькою – не завдають істотного деструктивного впливу
За ступенем ймовірності загрози	Малоймовірні небезпеки (потенційні), які потенційно не мають реальної можливості наступити; реальні
За стадією функціонування підприємства	На стадії створення підприємства; на стадії функціонування
За об'єктом посягань	Інформаційні; фінансові; матеріальні; загрози престижу, авторитету, іміджу підприємства
За суб'єктом загроз	Загрози зі сторони організованих злочинних угруповань; недобросовісних конкурентів; власних працівників; державних структур
За характером спрямування	Прямі; непрямі
За об'єктом спрямування	Виробничі секрети; відомості про фінансову діяльність; відомості про управління; відомості про клієнтів тощо
За тривалістю дії	Тимчасові; постійні
За рівнем суб'єктивного сприйняття	Неусвідомлені; із завищеним (заниженим) рівнем сприйняття; уявні; адекватні
За наявністю людського фактору	Пов'язані із діяльністю людини; не пов'язані із діяльністю людини
За характером відповідальності суб'єктів загроз за їх наслідки	Дисциплінарна, цивільно-правова, адміністративна, кримінально-правова
За видом збитків	Прямі; втрачена вигода

Джерело: складено автором.

Проаналізуємо основні види загроз комерційній таємниці підприємства.

Внутрішні загрози – загрози, джерела яких знаходяться всередині самого підприємства. Внутрішні загрози викликані недоліками та прорахунками у діяльності самого підприємства, що можуть призвести до втрати комерційної таємниці, а також ефективністю заходів, що вживаються для усунення причин та умов, що цим недолікам сприяють.

До основних факторів, які формують внутрішні загрози економічній безпеці, можна віднести наступні:

- недоліки в роботі з персоналом підприємства: некваліфікований підбір персоналу; відсутність корпоративної культури та виховання; відмова від проходження підвищення кваліфікації як умови для роботи із комерційною таємницею підприємства; невмотивованість персоналу до збереження секретів підприємства тощо.

- низький рівень організації роботи з документами, які містять комерційну таємницю підприємства (фінансовими документами, планами, звітами, кресленнями, технічною документацією, електронними носіями інформації тощо);

- невирішеність соціальних проблем працівників підприємства (низька заробітна плата, соціальна незахищеність, відсутність мотивації до праці тощо). Ці фактори впливають на формування лояльності до підприємства;

- плинність кадрів, відсутність досвідчених фахівців у сфері захисту комерційної таємниці, неефективна робота служби економічної безпеки;

- низький технічний рівень захисту від втрати інформаційних ресурсів підприємства.

До зовнішніх загроз відносять такі, джерела яких перебувають поза межами підприємства: промислове шпигунство; незаконні дії конкурентів (переманювання співробітників підприємства, які обізнані із комерційною таємницею підприємства, на більш високі посади, прямий підкуп співробітників представниками конкурентів, компрометація діяльності підприємства, компрометація керівників та окремих співробітників, укладання фіктивних цивільно-правових угод, паралізація діяльності підприємства шляхом використанням владних повноважень, засобів масової інформації тощо); протизаконні дії з боку кримінальних структур (вимагання та шантаж; викрадення комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем тощо); неправомірні дії працівників правоохоронних органів (безпідставне проведення перевірок; неправомірне вилучення документів, у тому числі, що містять комерційну таємницю тощо) тощо.

Практика підприємницької діяльності свідчить, що для суб'єкта господарської діяльності найбільшу небезпеку представляють зовнішні загрози, оскільки їх важко передбачити, а тому важко своєчасно вжити відповідних контрзаходів. Хоча існує і протилежна точка зору, заснована на тому, що внутрішні загрози безпосередньо пов'язані із «людським фактором» і представляють у зв'язку із цим найбільшу небезпеку для підприємства. Прихильники цієї теорії власну позицію обґрунтовують статистичними даними, відповідно до яких більше 3/4 збитків підприємство несе через пряму участь власних працівників у тих чи інших незаконних діяннях [8]. Також, неправомірні дії співробітників стали одними з головних причин внутрішніх інцидентів інформаційної безпеки на підприємствах, через які сталися витоки конфіденційних даних. До такого висновку прийшли фахівці аналітичної компанії B2B

International, проаналізувавши результати опитування Global corporate IT security risks 2013 спільно з «Лабораторією Касперського» [13]. Близько третини опитаних (32% у світі і стільки ж у Східній Європі) повідомили про витік, що стався через помилки співробітників.

Отже, проаналізувавши внутрішні загрози конфіденційності даних, які пов'язані з персоналом, можна побачити, що ігнорування цих загроз може призвести до серйозних збитків.

Розподіл загроз безпеці на описані два види (зовнішні та внутрішні) має практичну значимість, хоча в даний час вплив багатьох загроз носить транскордонний характер.

Загрози комерційній таємниці підприємства можна класифікувати також й за ступенем тяжкості спричинених наслідків: загрози з низьким, середнім та високим ступенем тяжкості наслідків.

Як правило, реалізація загроз з низьким ступенем тяжкості наслідків не справляє істотного впливу, навіть на поточну діяльність підприємства. Загрози, що спричиняють наслідки середнього ступеня тяжкості, передбачають додаткові витрати для відновлення попереднього становища і не потребують значних витрат часу. Найбільшу небезпеку для підприємства, його стратегічних програм та для персоналу представляють загрози з високим ступенем тяжкості наслідків. Їх здійснення, незалежно, чи працівниками підприємства, чи суб'єктами ззовні, може призвести до різкого погіршення фінансово-економічного стану підприємства та викликати можливе припинення його діяльності тепер або ліквідацію у майбутньому.

За ступенем ймовірності загрози комерційній таємниці можуть бути малоймовірні (потенційні) та реальні, відображаючи філософські категорії дійсності і можливості.

Потенційною загрозою є наявність існуючих або зародження нових небезпек у середовищі існування, вони створюють основу для формування передумов і можливостей нанесення шкоди. По суті, будь-яка апріорна небезпека є потенційною загрозою.

Реальна загроза – це небезпека, що остаточно сформувалася, коли для нанесення шкоди не вистачає одного або декількох факторів або умов.

Поділ загроз на описані дозволяє прогнозувати і попереджати можливість нанесення шкоди на самих ранніх стадіях формування загрози. При появі ж реальної загрози перед системою економічної безпеки підприємства виникає завдання створення таких умов, які дозволили б знизити дію загрози і перевести її в потенційну.

Важливе значення у безпеці підприємства має суб'єктивна сторона сприйняття загроз комерційній таємниці підприємства. Незважаючи на об'єктивну природу загроз, відображення людиною цього явища часто не співпадає з реальним становищем. Оцінка об'єктивно існуючої загрози завжди несе в собі елементи суб'єктивізму і вже в силу цього є спотвореним відображенням об'єктивної дійсності. Часом спотворення в сприйнятті загрози можуть мати гіпертрофований характер, або навпаки, загроза реально існує або формується, а суб'єкти безпеки можуть не знати про це, не усвідомлювати її характер. Тому для практики важливе значення має класифікація загроз за ступенем їх суб'єктивного сприйняття.

Під неусвідомленої загрозою мається на увазі загроза, яка реально існує, формується, але суб'єкти безпеки не знають про це і не очікують катастрофи, що насувається.

Під завищеною і заниженою загрозою розуміється об'єктивно існуюча загроза відповідно із завищеним або заниженим, аж до повного ігнорування, рівнем реальної небезпеки.

Під уявною загрозою розуміється помилкова, надумана, штучно сформована загроза при відсутності реального й достатнього приводу для цього.

Адекватна загроза відображає оптимальний випадок, коли реальні параметри загрози з достатньою точністю збігаються з її суб'єктивним сприйняттям. Причинами неадекватного сприйняття загроз можуть бути: обмеженість знань персоналу, відсутність необхідного обсягу достовірної інформації про події, низький рівень методів і оперативності обробки наявної інформації, відсутністю навичок прогнозування та передбачення наслідків тощо.

Важливе значення мають також особистісні особливості характеру і цільові світоглядні установки керівників та осіб, відповідальних за прийняття рішень у сфері безпеки підприємства. Формування неадекватного суб'єктивного сприйняття загроз може бути наслідком власної некомпетентності або помилки, або результатом цілеспрямованої діяльності інших осіб, які досягають власних цілей.

Також серед загроз комерційній таємниці підприємства можна виділити ті, які можуть виникнути на стадії створення підприємства і ті, що можуть перешкоджати нормальному функціонуванню підприємства. До першої категорії відносяться загрози, пов'язані із становленням суб'єкта як бізнес-одиниці (одержання реєстраційної та дозвільної документації; ліцензування господарської діяльності, набір персоналу, вихід на ринок тощо). Інші загрози, незважаючи на стале, можливо тривале, функціонування підприємства, також можуть вплинути на стійкість підприємства – від дестабілізації діяльності до повної руйнації.

За об'єктом спрямування за загрози поділяються на виробничі секрети; відомості про фінансову діяльність; відомості про управління; відомості про клієнтів тощо. Виділення таких видів загроз дозволяє цілеспрямовано виявити найбільш гострі, першорядні загрози, своєчасне запобігання яким дозволить підвищити ефективність діяльності щодо забезпечення економічної безпеки підприємства.

Усі охарактеризовані вище види загроз впливають на формування, розвиток і практичну діяльність системи економічної безпеки підприємства.

Суб'єкти загроз комерційній таємниці підприємства також повинні бути оцінені при організації системи економічної безпеки. Ними можуть бути всі, хто: або прямо чи опосередковано зацікавлені в конфіденційній інформації, що є у володінні підприємства (конкуренти, співробітники, партнери тощо); або шляхом заволодіння комерційною таємницею ставлять за мету дестабілізувати стан підприємства (наприклад, кримінальні структури або ті ж конкуренти); або визначають умови функціонування всіх або визначених підприємств (держава в особі органів державної влади, органи місцевого самоврядування, окремі посадові особи тощо).

За характером відповідальності суб'єктів загроз за їх наслідки: дисциплінарна, цивільно-правова відповідальність, адміністративна та кримінально-правова. Притягнення особи до відповідальності здійснюється в порядку, передбаченому діючим законодавством України.

Висновки та перспективи подальших розвідок. Отже, процес організації економічної безпеки підприємства полягає в єдності оцінювання ступеня вразливості економіки і можливості реалізації загрози. Якщо вразливість розуміти як залежність економіки від погіршення певних чинників з наступним підвищенням витрат на пристосування до нових умов, то за комбінації такої залежності з реальною загрозою виникають передумови до порушення економічної безпеки підприємства.

У процесі організації системи захисту комерційної таємниці підприємства потрібно враховувати наступні особливості:

по-перше, загроз, що можуть спричинити негативні наслідки, дуже багато, і не існує їх вичерпного або універсального переліку;

по-друге, забезпечення економічної безпеки підприємства – діяльність із виявлення, попередження та ліквідації фактів, явищ та процесів (загроз), що потенційно можуть завдати шкоди діяльності підприємства;

по-третє, в процесі організації системи економічної безпеки підприємства потрібно кожну виявлену загрозу піддавати аналізу по наступним параметрам: реальність загрози; її кількісна оцінка; засоби, необхідні для її нейтралізації. Результати співставлення одержаних даних є підставою для вжиття (або планування) конкретних заходів щодо ліквідації загрози або усунення негативних наслідків для підприємства у разі її реалізації.

Список літератури:

1. Кириченко О. А. Управління фінансово-економічною безпекою / О. А. Кириченко, С. М. Лаптєв, О. І. Захаров, П. Я. Пригунов; за ред. проф. В. С. Сідака. – К. : Дорадо-Друк, 2010. – 480 с.
2. Гнилицкая Л. В. Теоретико-методологические и прикладные основы обеспечения экономической безопасности субъектов хозяйственной деятельности. Монография / Л. В. Гнилицкая, А. И. Захаров, П. Я, Прыгунов. – К. : Дорадо-Друк, 2011. – 290 с.
3. Захаров О. Ю. Обеспечение комплексной безопасности предпринимательской деятельности. Теория и практика / О. Ю. Захаров. – М. : АСТ : Астрель ; Владимир : ВКТ, 2008. – 320 с.
4. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник / В. С. Сідак, В. Ю. Артемов. – К. : КНТ, 2007. – 160 с.
5. Ткачук И. Б. Коммерческая тайна: организация защиты, расследование посягательств / И. Б. Ткачук. – М. : Изд-во «Щит-М», 2000. – 168 с.
6. Ярочкин В. И. Коммерческая информация фирмы / В. И. Ярочкин. – М. : Ось-89, 1997. – 160 с.
7. Бабак В. П. Теоретичні основи захисту інформації: Підручник / В. П. Бабак. – К. : Книжкове вид-во НАУ, 2008. – 752 с.
8. Андрощук Г. А. Экономическая безопасность предприятия: защита коммерческой тайны. – Монография / Г. А. Андрощук, П. П. Крайнев. – К. : Издательский дом «Ин Юре», 2000. – 400 с.
9. Пескова Д. Р. Коммерческая тайна в системе экономических отношений: Монография / Д. Р. Пескова. – М. : МАКС Пресс, 2011. – 164 с.
10. Економічна безпека : навч. посіб. / за ред. З. С. Варналія. – К. : Знання, 2009. – 647 с.
11. Кадрова безпека суб'єктів господарської діяльності: менеджмент інсайдерами: Монографія / за ред. проф. Сідака В. С., проф. Мігус І. П. – Черкаси : ТОВ «МАКЛАУТ» – Черкаси, 2012. – 256 с.
12. Марущак А. І. Правові основи захисту інформації з обмеженим доступом: курс лекцій / А. І. Марущак. – К. : КНТ, 2007. – 208 с.
13. Сотрудники оказались главной угрозой для утечки информации из компании. [Электронный ресурс]. – Режим доступа: http://delo.ua/tech/sotrudniki-okazalis-glavnoj-ugrozoj-dlja-utechki-informacii-iz-k-213590/?supdated_new=1377788051. – название с экрана.

Личман Т. В.
Университет экономики и права «КРОК»

КЛАССИФИКАЦИЯ И АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ ПРЕДПРИЯТИЯ

Резюме
Исследована категория «угрозы» безопасности коммерческой тайне предприятия как фактор, определяющий механизм организации защиты коммерческой тайны в системе экономической безопасности предприятия.
Ключевые слова: коммерческая тайна, угрозы, экономическая безопасность предприятия.

Lichman T. V.
KROK University

CLASSIFICATION AND ANALYSIS OF ENTERPRISE COMMERCIAL SECRETS SECURITY THREATS

Summary
The category of «threats» to security of enterprise commercial secrets as a factor which determines the organization mechanism of commercial secrets protection in the system of enterprise economic security was investigated.
Key words: commercial secrets, threats, enterprise economic security.