Левчук Вікторія,
студентка ПДЕБ-31
юридичного факультету,
Західноукраїнський національний університет
Ронська О.Г
к.е.н, доцент кафедри безпеки та правоохоронної діяльності,
Західноукраїнський національний університет

УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ РЕСУРСІВ І КОМЕРЦІЙНИХ ДАНИХ ПІДПРИЄМСТВА

У сучасному інформаційному світі дані й відомості виступають найбільш вагомим активом. Підприємство, що оперує новими розробками, напрацьованими клієнтськими колами, продуманими фінансовими планами чи знаннями, які не підлягають розголошенню, набуває чинної переваги над опонентами. З огляду на це, захист комерційної інформації та ресурсів, що містять відомості, змінила свій статус із другорядної справи на ключовий вектор уваги. Зокрема, це стосується як комерційних структур, так і державних інституцій, що зумовлює актуальність дослідження.

Для початку зазначимо, що конфіденційна комерційна інформація – це відомості, які цінні саме завдяки своїй необізнаності серед широкого загалу. Їхньою ознакою є якраз той факт, що вони не перебувають у відкритому доступі, а отже, потребують запровадження відповідних механізмів для їхнього захисту. Ці дані охоплюють різні сфери, наприклад, інженерні рішення та бухгалтерська документація, перспективні кроки для покращення діяльності підприємства, дані про клієнтуру та підходи до маркетингу. Значимість цієї інформації полягає у гарантуванні коректного функціонування підприємства.

Доцільно щодо цього зазначають Н. Потапова та Л. Бушовська, які вказують про те, що захист даних та комерційної таємниці компанії слід розглядати як механізм забезпечення її стійкості за всіляких умов, зокрема тих, що є ворожими та походять із зовнішнього середовища. Це зовсім не залежить від того, яким чином зовнішні чинники впливають на роботу організації в аспектах інформації та технологій, а також від масштабів та характеру змін, що відбуваються всередині [1, с. 33].

Зокрема, суб'єкт господарювання, виступаючи власником відомостей, що становлять комерційну таємницю, має повноваження делегувати одному чи кільком особам функції щодо володіння, використання та розпорядження цією інформацією. Також він може встановлювати регламент опрацювання даних та порядок доступу до них, окрім того, визначати будь-які інші критерії доступу до комерційної таємниці. Проте важливо врахувати, що не вся наявна в розпорядженні інформація може бути наділена статусом комерційної таємниці, а отже, їй не може бути штучно обмежено доступ сторонніх суб'єктів, особливо державних контролюючих інстанцій.

Також зазначимо, що жоден чинний нормативно-правовий акт у межах національного законодавства не займається прямо урегулюванням поняття комерційної таємниці на підприємстві. Натомість, певні статті та положення як у вітчизняному, так і в міжнародному законодавстві містять норми, що стосуються поширення відомостей, які можуть вважатися комерційною таємницею, визначають її межі та встановлюють наслідки за несанкціоноване розголошення. Таким чином, з огляду на це, підприємства мають запроваджувати усі доступні методи для захисту інформаційних ресурсів, які охоплюють як різні рівні захисту, зокрема, фізичні бар'єри, програмні рішення, а також правові механізми.

Для забезпечення правового захисту комерційної таємниці або інформаційних ресурсів підприємства, кожному суб'єкту господарювання

варто мати відповідний пакет документації. Цей набір може охоплювати як засадничі установчі документи самого підприємства, так і внутрішні регламенти, що стосуються механізмів збереження зазначеної таємниці, включаючи чіткі настанови щодо процедур доступу. Також, на нашу думку, компанія має видати внутрішній розпорядчий документ, який формалізує порядок взаємодії обмеженого кола осіб із відомостями, що становлять комерційну таємницю, а також визначає правила роботи співробітників із цією інформацією. Заходи організаційного характеру націлені на те, аби обмежити доступ до важливої для бізнесу інформації тим особам, які не уповноважені нею оперувати. Це реалізується або через створення спеціалізованого підрозділу, або, у випадку менших фірм, шляхом призначення відповідальної особи чи декількох співробітників. Технічні заходи передбачають застосування різноманітних апаратних та програмних засобів, обладнання та інших технологічних рішень для захисту інформації, що має комерційну цінність для суб'єкта господарювання [2, с. 24].

Зокрема, ключовим моментом у збереженні комерційної таємниці виступає упорядкування та розподіл цієї інформації за категоріями чи ступенем важливості, надання можливості ознайомлення з нею лише певній групі співробітників, а також моніторинг її поширення. Доцільно в цьому контексті вказують О. М. Лобода та В. С. Фесенець: «Щодо кіберзахисту, то тут потрібні певні відомості, які слід надійно оберігати, адже їхнє зникнення може обернутися серйозними збитками для компанії. Методи та інструменти для забезпечення безпеки мусять унеможливлювати будь-які спроби несанкціонованого доступу. Успішність охорони даних полягає в тому, що витрати на впровадження заходів безпеки не можуть бути вищими за потенційні збитки від реалізації інформаційних ризиків» [3, с. 18].

Доцільно зазначити те, що у цій системі правоохоронні органи мають дві основні ролі. По-перше, це функція каральна, що полягає у розшуку, розслідуванні та притягненні до відповідальності тих, хто винен у неправомірному розголошенні комерційної інформації. Друга їхня місія – це превентивна та просвітницька робота з бізнесменами щодо потенційних загроз, надання практичної підтримки у налагодженні механізмів захисту, а також налагодження співпраці з комерційними структурами ще до моменту можливого інформаційного витоку.

Щодо цієї проблематики доцільно зазначають також і С. А. Пухир та Т. А. Немченко: «У світлі цифрової доби, охорона комерційної таємниці стає вирішальною місією для фірм, котрі прагнуть до високих позицій у конкурентному середовищі. З огляду на це, компаніям слід розробити дієвий механізм захисту комерційної таємниці та інформаційних ресурсів підприємства, який охоплюватиме як технологічні, так і управлінські кроки. Важливо також акцентувати увагу на вихованні у співробітників почуття обов'язку щодо нерозголошення конфіденційних даних, і постійно вдосконалювати цю систему захисту, адаптуючи її до динаміки зовнішніх обставин» [4, с. 298].

Отже, захист комерційної таємниці та інформаційних ресурсів підприємства – це не виключно правова чи технологічна проблематика, але й аспект організаційної етики та підзвітності. Навіть найкращі законодавчі акти та найновіші технічні інструменти не зможуть компенсувати правильного та сумлінного ставлення кожного члена колективу до збереження конфіденційності. В свою чергу, державні органи зобов'язані не лише вживати заходів щодо винних, а й формувати середовище, де захист інформаційного надбання стає невід'ємним елементом звичайної підприємницької діяльності.

ЛІТЕРАТУРА:

1. Потапова Н., Бушовська Л. Інформаційні ресурси системи забезпечення корпоративної безпеки бізнесу. *Вісник Хмельницького національного університету. Економічні науки.* 2023. № 6. С. 31-36.

2. Кравченко О. М. Удосконалення організаційно-правового забезпечення охорони конфіденційної інформації та комерційної таємниці бізнесу в Україні. *Екологічне право.* 2024. №1-2. С. 21-27.

3. Лобода О. М., Фесенець В. С. Застосування системи захисту інформаційних ресурсів підприємства. IV Всеукраїнська науково-практична інтернет-конференція «Сучасна молодь в світі ІТ» (Херсон-Кропивницький, 2023). 2023. С. 17-18.

4. Пухир С. А., Немченко Т. А. Стратегічні аспекти захисту комерційної таємниці на підприємстві. Матеріали VI Міжнародної науково-практичної конференції «Конкурентоспроможна модель інноваційного розвитку економіки України» (м. Кропивницький, 7-8 грудня 2023 року). 2023. 297-298.