2. Revolut's Growth Strategy Explained, 2021. URL: https://www.paymentgenes.com/all-about-payments-videos/revoluts-growth-strategy-explained
3. Revolut | Neo-Bank Strategy Deep Dive. Complimentary Research (2020). URL: https://whitesight.net/reports/revolut-neo-bank-deep-dive/
4. PwC Ukraine advises NovaPay on its expansion into European markets, 2023. URL: https://www.pwc.com/ua/en/press-room/2023/pwc-ukraine-advises-novapay.html

Фомічов К.С., кандидат юридичних наук, доцент
Турта Р.А., ст. гр. УФЕБ – 22 М
Центральноукраїнський національний технічний університет

ХАРАКТЕРИСТИКА ОСНОВНИХ ЗАХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗБЕРЕЖЕННЯ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ПІДПРИЄМСТВІ

В промислово розвинених країнах управління комерційною таємницею лежить у сфері відповідальності як окремих осіб, так і різних внутрішньофірмових підрозділів. Проте далеко не всі вітчизняні компанії мають служби безпеки, тому особливу увагу до збереження конфіденційності варто приділяти при укладанні трудових угод між адміністрацією та працівниками. Це момент, де відображаються індивідуальні зобов'язання працівників щодо збереження комерційної таємниці.

За дослідженнями західних фахівців, 25% працівників підприємств готові за будь-яких обставин зрадити інтересам фірми, 50% можуть це зробити залежно від ситуації, тоді як лише 25% залишаються вірними фірмі [1].

Основні втрати для підприємства включають:

- Зменшення можливостей продажу ліцензій на власні наукові розробки.
- Втрату пріоритету у досліджуваних сферах науково-технічного прогресу.
- Зростання витрат на переорієнтацію діяльності дослідницьких підрозділів.

Точний обчислення загального обсягу збитків часто важкий індикативний процес через відсутність достовірних даних. Тому експертна оцінка втрат підприємства, викликаних порушенням вимог захисту інформації, є досить узагальненою.

Компенсація цих збитків вимагає значних додаткових витрат, що впливає на ефективність виробництва та можливість успіху в конкурентній боротьбі. Тому питання захисту комерційної таємниці стає предметом все більш детального вивчення заходів забезпечення конфіденційності інформації на підприємстві.

Ці заходи можна умовно класифікувати на зовнішні та внутрішні, які, в свою чергу, розділяються на правові, організаційні, технічні та психологічні. Деякі джерела також виокремлюють страхування комерційної таємниці від розголошення.

Крім того, захист комерційної таємниці передбачає:

- Визначення інформації, що містить комерційну таємницю і термін її дії.
- Регулювання доступу співробітників і відряджених осіб до цієї інформації.
- Організацію роботи з документами та грифом "КТ".
- Забезпечення збереження документів, справ і видань з грифом "КТ".
- Визначення відповідальності за розголошення відомостей та втрату документів КТ.

Контроль за обліком, копіюванням, зберіганням та використанням документів, справ і видань з грифом "КТ" покладається на уповноважені служби безпеки. Перелік і обсяг інформації, що вважається комерційною таємницею підприємства, строки конфіденційності та умови доступу до неї встановлюються керівником організації. Керівник може залучати спеціалістів-аналітиків для цієї роботи.

Основна мета захисту конфіденційної інформації полягає в запобіганні її поширенню серед конкурентів. У деяких випадках важливо захищати також "чужі" комерційні секрети, довірені підприємству. Відсутність такого захисту може ускладнити залучення вигідних партнерів та клієнтів.

Заходи щодо встановлення захисту комерційної таємниці включають:

– розробка стандартів внесення інформації до переліку комерційної таємниці на підприємстві;

– розробку і розповсюдження інструкцій з метою дотримання збереження конфіденційної інформації;

– встановлення обмеженого доступу до носіїв інформації з комерційною таємницею;

– використання організаційних, технічних та інших заходів захисту інформації;

– здійснення контролю щодо дотримання режиму секретності та охорони комерційної таємниці.

Менеджер, як і інші співробітники, повинен підписати зобов'язання щодо нерозголошення комерційної таємниці при вступі на роботу. Він має доступ до різних джерел інформації, таких як організація зустрічей, переговорів, обробка кореспонденції та інше.

Менеджер відіграє ключову роль у збиранні інформації, тому йому важливо проявляти обережність у розмовах з партнерами чи клієнтами, де будь-яка інформація може бути значущою.

Для обмеження доступу до комерційної таємниці керівник видає спеціальний наказ щодо введення до "Переліку відомостей, що вважаються комерційною таємницею підприємства". Співробітники повинні ознайомитись з цим наказом та додатками до нього.

Перелік відомостей, що становлять комерційну таємницю підприємства, може включати різноманітну інформацію: від обсягів кредитів та контрагентів до маркетингових досліджень та іншого.

Отже, захист комерційної таємниці підприємства безпосередньо впливає на його інформаційну та економічну безпеку.

Література:

1. Бондар О.В. Ситуаційний менеджмент. Навч. Посібник. К.: Центр учбової літератури, 2012. – 388 с.

2. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В.М. Фурашев // Інформація і право: науковий журнал. – К.: НДЦПІ НАПрН України, 2012. – № 1(4). – С.46– 56.

Ушакова Я.В., здобувач гр. МЕ-22М
Музиченко А.С., докт. екон. наук., проф.
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

ОСОБЛИВОСТІ УПРАВЛІННЯ АКЦІОНЕРНИМ КАПІТАЛОМ БАНКІВСЬКИХ УСТАНОВ

Управління капіталом передбачає безперервний процес оптимізації його використання як на стратегічному, так і на операційному рівнях із застосуванням різних стратегій, методів та інструментів управління. Керуючи банківською установою менеджер повинен знаходити баланс між ризиком і достатністю капіталу, дотримуючись економічних нормативів, встановлених Національним банком України.

Управління акціонерним капіталом у банківських установах обертається навколо виконання різноманітних завдань, таких як: