

**Коврига Р. Є.**

*Дніпровський національний університет імені Олеся Гончара (Україна)*

## **ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ЯК СКЛАДОВИЙ ЕЛЕМЕНТ ЕКОНОМІЧНОЇ БЕЗПЕКИ**

Для будь-якого періоду розвитку суспільного виробництва характерним є постійне розширення сфери виникнення ризику на підприємстві. У свою чергу результатами ризикових ситуацій стає збільшення розміру можливих негативних наслідків, які слід розглядати як своєрідну плату за свободу підприємництва.

У чому виражається можливість негативної реалізації ризику?

Розмір можливих негативних наслідків виражається у виникненні будь-якого збитку, зокрема, по-перше, слід розглядати шкоду у вигляді втрачених вигод при отриманні доходу, по-друге, в можливості втрати власного капіталу. Саме ці факти змушують задуматися і поставитися дуже серйозно до проблеми наявності ризиків та управління ними. Тим більше це актуально в процесі розвитку суспільного виробництва, супроводжуваного кризовими проявами на всіх рівнях економічного узагальнення. У зв'язку з цим в майбутньому більш конкурентоспроможними і затребуваними в суспільстві повинні стати ті нововведення, технології і продукти, які будуть забезпечувати менший ступінь ризику – меншу ймовірність і розмір можливих збитків, втрачених вигод або втраченого капіталу.

Таким чином, зниження ризику пов'язано, по-перше, з пошуком і впровадженням нових продуктів, послуг та технологій, виробництво яких не веде до збільшення ризику. По-друге, воно можливе за рахунок управління ризиком, яке передбачає його виявлення і оцінку, а також використання таких процедур і методів управління, які знижували б можливі ризики. [2]

Інформаційна безпека – це стан захищеності інформаційного середовища підприємства, що забезпечує його функціонування і розвиток в інтересах його персоналу. Складність цього поняття полягає в тому, що для формування вимог до безпеки інформаційного об'єкта підприємства важко визначити його внутрішні властивості та структуру. Навіть саме визначення інформації, в даний час дуже неоднозначне і суперечливе. Таким чином сформувані поняття безпеки предмета, який виступає інформаційним джерелом, на підставі його внутрішньої структури

і внутрішніх властивостей не представляється можливим. Тому параметрами для інформаційної безпеки об'єкта підприємства виступають такі складові:

Конфіденційність інформації – такий стан інформації, при якому визначаються певні права доступу до неї окремих об'єктів підприємства.

Цілісність інформації – блокування несанкціонованих змін інформації.

Доступність інформації – не приховувати інформацію від користувачів з правами доступу.

Потрібно також звернути увагу на те, що всі складові являють собою тільки зовнішні дії по відношенню до інформації: призначення прав доступу до інформації; блокування несанкціонованих змін інформації; уникнення приховування інформації від користувачів з правами доступу.

Головною метою будь-якої системи інформаційної безпеки є перш за все забезпечення постійного функціонування об'єкта, запобігання загрози його безпеки, захист інтересів від незаконного втручання і т.д.

Також метою системи інформаційної безпеки є покращення якості послуг, що надаються, і гарантій безпеки майнових прав та інтересів клієнтів. Одним з найбільш дієвих методів забезпечення інформаційної безпеки є організаційно-технічні методи, які направлені на створення і вдосконалення системи забезпечення інформаційної безпеки. Загроза для інформації виражається в порушенні її цілісності, конфіденційності, повноти і доступності. Джерелами загроз можуть виступати конкуренти, порушники, корупціонери, адміністративно-управлінські органи.

Розробка політики інформаційної безпеки – питання досить суттєве. Від ретельності її опрацювання буде залежати дієвість всіх інших рівнів забезпечення інформаційної безпеки – процедурного і програмно-технічного.

Перший напрямок інформаційної безпеки підприємства – підприємству слід розробити просту систему класифікації ступеня конфіденційності оброблювальних матеріалів [1].

Другий напрямок інформаційної безпеки підприємства – потрібно постійно виконувати з персоналом роботу щодо правил використання конфіденційної інформації.

Третій напрямок інформаційної безпеки підприємства – зобов'язати визначати рівень таємності документу на ту особу, яка його розробляла. Ця людина в подальшому може змінювати ступінь таємності цієї інформації.

**Список використаних джерел:**

1. Ганущак Т. В. Фінансова безпека бізнесу : Навчальний посібник. Київ: *Департамент поліграфії Університету* . 2016. 266 с.
2. Древаль Ю. Д. Безпека особистості як фактор сучасних державно управлінських відносин. *Наукові записки Інституту законодавства Верховної Ради України*. С. 123–127.
4. Гринько Т.В., Алещенко В.І. Вплив та взаємозв'язок ефективності та економічної безпеки підприємства. *Науковий вісник Міжнародного гуманітарного університету, Серія: Економіка і менеджмент*, 2020. Видавничий дім «Гельветика». Вип. 42. С. 4-11.

**Ласточкіна В. В., Димарчук К. І.**

*Дніпровський національний університет імені Олеся Гончара (Україна)*

**БЕЗПЕКА КАДРОВОЇ ПОЛІТИКИ ПІДПРИЄМСТВА**

Успішне функціонування підприємства в умовах ринкової економіки передбачає забезпечення ефективної системи заходів економічної безпеки. Економічна безпека є сукупним поняттям, тому що об'єднує різні функціональні складові. На думку більшості провідних економістів в цій предметній області серед складових економічної безпеки виділяються інформаційна, фінансова, техніко-технологічна, інтелектуальна, політико-правова, кадрова. Ефективне забезпечення кадрової безпеки на підприємстві виступає одним з пріоритетів в досягненні стабільності і процвітання не лише окремого підприємства або групи підприємств, а й економічної системи держави в цілому.

Одним з найважливіших пріоритетів будь-якого підприємства є ефективна кадрова політика, спрямована на створення єдиної професійної команди працівників, які мають необхідний потенціал для реалізації стратегічних цілей, а також збереження накопиченого інтелектуального капіталу. Тому для переважної більшості зацікавлених керівників стоїть проблема щодо створення та забезпечення такої кадрової безпеки, при якій індивідуальні та специфічні запити окремо взятого підприємства зможуть бути задоволені [1].

Забезпечення кадрової безпеки – одна з найважливіших систем сучасної організації. Система безпеки – це комплекс організаційних і технічних заходів,