

ІНТЕЛЕКТУАЛЬНА БЕЗПЕКА ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

О. С. Марченко, д. е. н., проф.
проф. кафедри економічної теорії
Національного юридичного університету
імені Ярослава Мудрого

Провідними ресурсами економіки знань є ресурси інтелектуальні, що обумовлює необхідність перегляду підходів, що склалися, до визначення пріоритетних об'єктів, умов та напрямів забезпечення економічної безпеки на макро- і мікроекономічних рівнях.

В інформаційному суспільстві у структурі об'єктів економічної безпеки зростає значущість інтелектуальних ресурсів, захищеність яких є базовою умовою забезпечення розвитку національної економіки. Виходячи з цього, в сучасних умовах забезпечення інтелектуальної діяльності як діяльності з продукування, обміну, використання інтелектуальних ресурсів, виступає однією з пріоритетних складових економічної безпеки.

Інтелектуальна безпека – це захищеність інтелектуальних ресурсів соціально-економічного розвитку, їх продукування, обміну, використання на макро- та мікроекономічних рівнях.

За об'єктним критерієм інтелектуальна безпека – це захищеність знань як інтелектуальних ресурсів суспільства, що охоплює забезпечення працівників знань та їх інтелектуальної праці; інтелектуального продукту; інтелектуальної власності, інтелектуального капіталу. Основу інтелектуальної безпеки складають науковий і освітній потенціали суспільства, господарюючого суб'єкту, індивідуума.

Складовими інтелектуальної безпеки є:

1) безпека інтелектуальних трудових ресурсів як носіїв знань – це такий стан їх захищеності, що забезпечує ефективну реалізацію неявних індивідуальних і колективних знань у процесі діяльності суб'єктів господарювання, запобігає втратам знанневих ресурсів внаслідок опортуністичної поведінки працівників;

2) безпека нематеріальних активів як об'єктів права інтелектуальної власності фірми, до яких належать: майнові і немайнові права, об'єкти промислової власності, створена і накопичена фірмою база знань – все це носії організаційних знань. Це стан їх захищеності від зовнішніх та внутрішніх загроз, пов'язаних з можливістю їх втрати, несанкціонованого копіювання, використання конкурентами, плагіату та ін.;

3) безпека інтелектуального капіталу як стан захищеності інвестицій фірми у знаннєві ресурси. У цьому контексті безпека інтелектуального капіталу є однією з форм інвестиційної безпеки фірми. Захист інтелектуального капіталу фірми – це сукупність заходів щодо його збереження та ефективної реалізації;

4) безпека руху знань в організації, що охоплює створення, залучення, розповсюдження (дифузю), оволодіння знаннями, перетворення, обмін, збереження, використання знань як їх об'єктивізація у продукції та послугах фірми;

5) кібербезпека – захищеність інформаційно-комунікаційних технологій (ІКТ). Кіберзлочинність як використання новітніх ІКТ, спрямоване проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання ними є загрозою інтелектуальній безпеці. Це правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушення, пов'язані з комп'ютерами; правопорушення, пов'язані із змістом; правопорушення, пов'язані з порушенням авторських та суміжних прав.

Отже, на рівні фірми інтелектуальна безпека – це стан захищеності носіїв і руху знань. Захист носіїв знань, метою якого є забезпечення накопичення і ефективної реалізації їх потенціалу, спрямовано на запобігання загрозам, пов'язаним з їх формуванням і функціонуванням. Його складовими відносно такого носія знань як працівники є захист інтелектуальної праці, що охоплює певні техніко-технологічні, економічні, організаційні, культурологічні заходи; освітній захист як запобігання загрозам ефективного навчання та самонавчання працівників знань; захист кар'єри – сукупність заходів, що забезпечують просування працівника в організації адекватно рівня його компетенції тощо. Здійснення захисту інтелектуальних працівників – носіїв специфічних неявних знань сприяє, з одного боку, подоланню загроз їх опортуністичної поведінки, як-то: несанкціоноване використання знаннєвих ресурсів, порушення конфіденційності, розголошенням комерційної таємниці, промисловий шпідіаж та ін., з іншого боку, збереженню інтелектуальних трудових ресурсів, запобігання їх переходу до конкурентів.

Захист руху знань в організації здійснюється шляхом визначення і подолання загроз, серед яких: передавання недостовірної чи застарілої інформації, несанкціоновані бар'єри щодо передачі-отримання знань, недоброчесна конкуренція на ринку знань, зловживання монопольним становищем відносно певних знаннєвих ресурсів тощо.

Серед інтернальних загроз безпеці інтеграції знань варто виділити такі: 1) недостатній рівень специфікації прав власності щодо інтелектуального продукту; 2) інституціональна невизначеність процесів інтеграції знань у межах фірми. Негативними наслідками цього є опортуністична поведінка працівників фірми як носіїв знань і учасників їх внутрішньофірмового руху, «відплив умів», перетворення інвестицій фірми у інтелектуальні активи на неповоротні втрати.

Найважливішою проблемою є коригування і подолання опортуністичної поведінки працівників у формі ухиляння і вимагання, що складає загрозу інтелектуальній безпеці фірми. З одного боку, творчу діяльність неможливо контролювати адміністративними методами, а використання командної форми організації інтелектуальної праці ще більше

ускладнює зовнішній контроль виконання трудових функцій. Тому цілком реальною є ситуація ухиляння – приховане невиконання або недостатній рівень виконання найманими працівниками умов трудового договору. З іншого боку, залежність фірми від специфічних та інтерспецифічних інтелектуальних трудових ресурсів породжує можливість вимагання з боку її співробітників кращих умов праці, вищої оплати, пільг і доплат, не пов'язаних з реальними результатами їх діяльності.

Інвестиціям фірми в людський капітал властиві значні ризики, пов'язані з реальною загрозою їх перетворення на безповоротні витрати. Наприклад, цілком типовою є ситуація, коли витрати фірми на адаптацію і навчання працівників не дають очікуваного ефекту внаслідок їх опортуністичної поведінки. Так, корпоративна освіта сприяє зростанню творчого потенціалу специфічних інтелектуальних трудових ресурсів фірми. Однак, внаслідок звільнення працівників або їх опортуністичної поведінки та безвідповідального ставлення до навчання, є загроза, що знання можуть бути втрачені фірмою, а її витрати на професіональне зростання працівників перетворяться на втрати. Суттєвою загрозою інтелектуальній безпеці є несанкціоноване використання та розкриття конфіденційної інформації.

Серед напрямків подолання загроз інтелектуальній безпеці необхідно виокремити наступні:

1) розвиток культури фірми як інтелектуальної організації, яка базується на правилах: вдосконалювання, власність, розуміння, підхід «можу зробити», чесність, доступність, професіоналізм;

2) інвестиції в закріплення і збереження висококваліфікованих фахівців фірми, наприклад, капіталовкладення у створення соціальної інфраструктури, що забезпечують підвищення якості життя (житло, відпочинок, медичне обслуговування);

3) трансформація індивідуальних знань у колективні, що забезпечує фірмі певний рівень незалежності від можливих втрат знань, внаслідок опортуністичної поведінки чи звільнення працівників фірми. Колективне знання (знання груп людей і організації в цілому) становить собою ключові компетенції як згустки знань і навичок що забезпечують конкурентоспроможність фірми і дозволяють у сконцентрованому виді виявити генетичні джерела її виживання і розвитку в конкретному діловому середовищі. Трансформація знань з метою забезпечення інтелектуальної безпеки фірми охоплює такі головні напрямки: формалізація знань на підставі підготовки різних методик, наукових обґрунтувань, проектів, розробок, статей і навчальних матеріалів, що становлять базу знань, яка належить фірмі; перетворення інтелектуального продукту найманих працівників на об'єкти інтелектуальної власності фірми; поширення знань в організації у процесі внутрішньофірмового навчання, формування культури організації, що самонавчається, з метою перетворення окремих елементів, які становлять зміст фірмово-специфічного людського капіталу, на колективне знання;

4) мотивація носіїв знань на базі:

а) застосування принципів організації оплати інтелектуальної праці: індивідуалізованість, багатофакторність, гарантованість, гнучкість і комплексність;

б) реалізації у процесі забезпечення інтелектуальної безпеки фірми специфічних функцій оплати праці, а саме:

(1) функції, яка полягає у закріпленні (збереженні) глибоко спеціалізованих інтелектуальних трудових ресурсів, їх «монополізації» фірмою. Висококваліфіковані працівники є і головною конкурентною перевагою фірми, і її основним обмежувальним ресурсом. Використання оплати праці як інструмента закріплення (збереження) специфічних і інтерспецифічних інтелектуальних трудових ресурсів фірми – дієвий засіб подолання загроз інтелектуальній безпеці фірми;

(2) капіталоутворюючої функції стосовно фірмово-специфічного людського капіталу. Капіталоутворюючий потенціал оплати праці фахівців полягає в можливості фінансування за її рахунок підвищення їх професіонального рівня. Витрати фірми на навчання і підвищення кваліфікації працівників як структурний елемент витрат на оплату праці (зокрема, на соціальні виплати – соціальний пакет працівників знань) є інвестиціями у фірмово-специфічний людський капітал. Капіталоутворююча функція оплати праці відбиває тісний взаємозв'язок інтелектуальних трудових ресурсів фірми і фірмово-специфічного людського капіталу як структурного елемента інтелектуального капіталу фірми. Її значимість зумовлена загальносвітовою тенденцією зростання інтелектуального компонента у відтворенні робочої сили;

5) створення інституційних умов інтелектуальної безпеки організації, розробка і впровадження системи внутрішньофірмових правил і процедур руху знань, зокрема, специфікація прав власності щодо інтелектуального продукту працівників фірми;

б) застосування технологій управління знаннями, що забезпечують сполучення індивідуалізації, волі, самостійності, участі в управлінні, довіри, співробітництва і культури.

Забезпечення інтелектуальної безпеки фірми є функцією адміністраторів знань (knowledge administrations), для яких управління знаннями – це професійна діяльність, спрямована на створення техніко-технологічних, організаційно-економічних, мотиваційних, інституційних умов і чинників ефективного використання інтелектуальних ресурсів організації.