

2. містить всі рівні (регулярні публічні закупівлі, дружні до інновацій; стратегічні публічні закупівлі; публічні закупівлі НДР) та типи публічних закупівель (інноваційні публічні закупівлі; публічні закупівлі інновацій; публічні закупівлі для інновацій; публічні закупівлі інноваційних рішень; передкомерційні публічні закупівлі; інноваційні партнерства);

3. передбачає стимули не лише для радикальних, а й для поступових інновацій, тобто враховує позитивний вплив всіх видів публічних закупівель на інновації.

Враховуючи відсутній в Україні досвід стимулювання інновацій через систему публічних закупівель, напрямом подальших досліджень має стати аналіз міжнародного досвіду використання системи публічних закупівель для стимулювання інновацій та розробка відповідних рекомендацій з урахуванням соціально-економічного становища економіки України.

УДК 658:589:656.2

Гарбузюк К.Г., к.ю.н., декан факультету № 2

ORCID ID: <https://orcid.org/0000-0002-6714-5074>

Ткаченко С.А., к.е.н., доцент, завідувач кафедри соціальних та економічних дисциплін факультету № 2

ORCID ID: <https://orcid.org/0000-0002-5816-4185>

Харківський національний університет внутрішніх справ, м. Харків, Україна

КОНЦЕПТУАЛЬНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ СУБ'ЄКТА ГОСПОДАРЮВАННЯ

Концепція економічної безпеки представляє собою основні напрями, порядок і умови практичного вирішення основних завдань захисту комерційних інтересів і майнових прав суб'єкта господарювання, його структурних підрозділів (підприємств, об'єднань), членів їх керуючих органів та осіб, що є носіями комерційної інформації щодо фінансово-господарської діяльності від протиправних дій і недобросовісної конкуренції.

Головною метою системи економічної безпеки є забезпечення стійкого функціонування суб'єктів господарювання та запобігання загрозам їх безпеці, захист законних інтересів об'єктів безпеки від протиправних зазіхань, недопущення втрати прав власності на майно, необхідне для здійснення статутної діяльності, його знищення, розголошення, втрати, витоку, спотворювання та знищення інформації з обмеженим доступом, порушення роботи технічних засобів.

Крім того, додатковими цілями є:

- визначення шляхів реалізації заходів, що забезпечують необхідний рівень критеріїв захищеності суб'єктів господарювання;
- підвищення іміджу суб'єкта господарювання, проведення організаторської роботи з пошуку нових контрагентів, забезпечення високої якості торговельної, виробничої та інших видів діяльності.

У свою чергу, завданнями системи економічної безпеки є:

- моніторинг, прогнозування, своєчасне виявлення і усунення загроз безпеці системі господарювання структурних підрозділів, причин і умов, що сприяють нанесенню моральної та матеріальної шкоди, порушенню їх функціонування і розвитку;
- віднесення інформації до категорії обмеженого доступу (комерційної та конфіденційної інформації), а також інших інформаційних ресурсів - до різних рівнів вразливості і таких, що підлягають збереженню;
- створення механізму та умов оперативного реагування на загрози економічній безпеці і прояви негативних тенденцій у функціонуванні структурних підрозділів;
- ефективне запобігання посяганням на ресурси структурних підрозділів шляхом застосування правових, організаційних та інженерно-технічних заходів для досягнення необхідного рівня безпеки;
- застосування нормативно-правового механізму з метою локалізації (мінімізації) негативного впливу наслідків порушення економічної безпеки;
- створення уніфікованого інформаційного забезпечення щодо стану загроз фінансово-господарської діяльності суб'єкта та його структурних підрозділів.

Основна мета захисту схоронності науково-технічної інформації - це можливість подальшого використання юридичними й фізичними особами результатів своїх розробок, одержання комерційної вигоди від їхнього використання, продажу тощо.

На нашу думку, захист прав схоронності науково-технічної інформації - заходи щодо визнання прав, їхнього відновлення, припинення порушень, застосування до порушників заходів відповідальності, а також механізм практичної реалізації цих мір.

Право інтелектуальної власності становлять особисті немайнові права інтелектуальної власності й (або) майнові права інтелектуальної власності, зміст яких щодо певних об'єктів права інтелектуальної власності визначається законодавством.

Для ефективного захисту комерційної організації щодо схоронності науково-технічної інформації необхідно:

- визначити ресурси, що підлягають захисту;
- провести оцінку можливого збитку від витоку конфіденційних відомостей і класифікацію інформації за ступенем важливості;
- виявити всі види носіїв інформації, що підлягають захисту;
- визначити й оцінити потенційні умови уразливості інформації;
- створити комплексні міри щодо безпеки науково-технічної інформації.

Інформаційні активи, що підлягають захисту:

- документи стратегічного розвитку;
- прогнози щодо розвитку бізнесу;
- внутрішні документи конкурентного аналізу;
- аналітика ринків;
- внутрішні накази й розпорядження;
- матеріали кадрового діловодства;

- списки внутрішніх телефонів і електронних адрес співробітників;
- посадові інструкції по окремих підрозділах;
- дані системи по роботі із клієнтами;
- опис «ноу-хау» і технологічних процесів;
- проектні дані (схеми, креслення, розрахунки, плани робіт);
- звіти щодо реалізації проектів;
- звіти щодо контролю якості;
- схеми внутрішніх бізнес процесів;
- схеми інформаційних потоків і комунікацій;
- архітектура інформаційної системи;
- активаційні коди на ліцензійне програмне забезпечення.

Загрози негативного впливу на бізнес витоку науково-технічної інформації:

- падіння лояльності клієнтів;
- зниження числа нових і відтік існуючих замовників;
- втрата довіри постачальників і партнерів;
- ослаблення позицій у конкурентній боротьбі;
- втрата технологічних секретів;
- звільнення співробітників;
- зниження котирувань акцій і втрата довіри інвесторів;
- зниження вартості бренду;
- вплив на рейтинги компанії;
- погіршення іміджу компанії;
- санкції контролюючих органів;
- судові розгляди;
- необхідність витрат на усунення наслідків.

Види порушень прав науково-технічної інформації:

- недотримання договірних умов використання інформаційних об'єктів і (або) об'єктів суміжних прав;
- використання інформаційних об'єктів і об'єктів суміжних прав з обходом технічних засобів захисту або з піддробкою інформації й (або) документів щодо управління правами;
- створення загрози неправомірного використання об'єктів авторського права й (або) суміжних прав;
- здійсненні дій, які належать до несумлінної конкуренції;
- інші порушення особистих немайнових і майнових прав.

Способи захисту схоронності науково-технічної інформації:

- визнання права;
- визнання договору недійсним;
- припинення дії, що порушує право;
- відновлення положення, що існувало до порушення права;
- примусове виконання зобов'язань у натуральному виразі;
- зміна правовідносин;
- припинення правовідносин;
- відшкодування збитків та інші способи відшкодування майнової шкоди;

- відшкодування моральної (немайнової) шкоди;
- визнання незаконними рішення, дії або бездіяльності органа державної влади.

Додатково, варто застосувати:

- запобіжні заходи щодо порушення прав і схоронності відповідних доказів;
- припиненню пропуску через митний кордон України товарів, імпорту або експорту яких здійснюється з порушенням прав схоронності науково-технічної інформації;
- вилучення із цивільного обороту товарів, виготовлених або уведених у цивільний оборот з порушенням прав схоронності науково-технічної інформації;
- застосування разового грошового стягнення замість відшкодування збитків за неправомірне використання об'єкта прав науково-технічної інформації;
- опублікування в засобах масової інформації відомостей про порушення права схоронності науково-технічної інформації і зміст судового рішення про таке порушення.

Для подолання загроз витоку науково-технічної інформації вводиться відділ контролю науково-технічних розробок (КНТР), що є структурним підрозділом служби забезпечення безпеки бізнесу.

Основні завдання відділу КНТР:

- активізація, стимулювання інноваційної діяльності наукових колективів;
- координація підприємницької діяльності, а також представлення й захист спільних інтересів учасників інноваційної діяльності щодо створення умов для комерціалізації результатів науково-дослідних і науково-технічних програм і проектів;
- розробка ефективних механізмів управління й фінансування інноваційного підприємництва;
- розвиток інноваційної інфраструктури;
- оцінка й пропозиції щодо розвитку інноваційного потенціалу;
- організація й проведення оцінки корисного потенціалу науково-технічних розробок;
- бізнес-тестування науково-технічних розробок;
- сприяння в пошуку партнерів;
- впровадження результатів наукових досліджень, що мають комерційний потенціал;
- розробка механізму технологічного трансферу науково-технічних розробок.

Відповідальність за порушення механізмів схоронності й оцінки ризиків витоку науково-технічної інформації застосовується у формі цивільно-правової, адміністративної й кримінальної відповідальності, а також можуть застосовуватися фінансові санкції.