2. Боднарчук О. Г. Сінгапурська модель боротьби з корупцією – приклад застосування ефективної антикорупційної стратегії в Україні / [Електронний ресурс]. – Режим доступу: http://www.lsej.org.ua/2_2014/13.pdf
3. Невмержицький Є. В. Корупція в Україні: причини, наслідки, механізми протидії [Текст]: [монографія] / Є. В. Невмержицький; Академія прокуратури України. – К.: КНТ, 2008. – 368 с.

Якубівська Ю. Є.
к.е.н., доцент кафедри фінансово-економічної безпеки та інтелектуальної власності ЮФ ТНЕУ

ПОБУДОВА СИСТЕМИ ІНТЕЛЕКТУАЛЬНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

На сучасному етапі розвитку національної безпеки України особливої актуальності набуває дослідження проблеми забезпечення інтелектуальної безпеки підприємства, яка забезпечує ефективність його діяльності.

Досліджуючи етимологічні аспекти категорії «інтелектуальна безпека», варто зазначити, що це дане поняття включає в себе такі складові, як інтелектуальний капітал, інтелектуальний потенціал та інтелектуальна власність. У деяких іноземних джерелах інтелектуальна безпека розглядається в якості рівнозначного поняття інтелектуальній власності [1, с. 12], що на думку автора, не є достатньо обґрунтованим. В інших – як елемент охорони та захисту результатів розумової діяльності людини, а також раціонального володіння, користування, розпорядження і підвищення якості розумових здібностей людей, що потенційно визначають їх сферу діяльності [2, с. 6].

Основоположною метою забезпечення інтелектуальної безпеки на підприємстві слід вважати гарантію сталої та максимально результативної його діяльності на відповідний час та перспективи розвитку та підвищення ефективності діяльності в майбутньому. Першорядною умовою забезпечення інтелектуальної безпеки підприємства є спроможність протистояти небезпекам, які вже існують та які потенційно можуть виникнути та завдати шкоди підприємству, і відповідно, за яких підприємство може понести істотні збитки.

Коли постає загроза інформаційної безпеки для підприємства, керівництво часто думає, в першу чергу, як воно може захистити свої оперативні дані та систему інформаційних технологій. Тим не менш, даний аспект відіграє важливу роль в захисті інтелектуальної власності на підприємстві – в контексті захисту творчих ідей, інновацій та винаходів.

Права інтелектуальної власності та інтелектуальна безпека стимулюють розвиток інноваційної діяльності, досліджень та відкриттів. Метою таких прав є надання законним власникам винаходів або творчих ідей ексклюзивної можливості отримання прибутку від нього протягом певного періоду часу. Це означає, що правовласник має право використовувати відповідний об’єкт інтелектуальної власності для особистої вигоди і контролювати, як інші можуть його використовувати. Кожен тип об’єктів має різні вимоги для набуття, захисту, а також забезпечення інтелектуальної безпеки на підприємстві в контексті охорони та захисту від посягання на нього третіх осіб. Виокремимо деякі з них, які найчастіше підпадають під посягання на систему інтелектуальної безпеки підприємства:

1. Патенти: використовуються для захисту винаходів (таких як машини, процеси і конструкції) на протязі відповідного періоду часу. Патент є техніко-економічним документом, що визначає право інтелектуальної власності на відповідний об'єкт.

2. Авторські права: використовуються для захисту творів мистецтва, музики, відео, комп'ютерних програм, книг та подібних творчих робіт протягом визначеного періоду часу.

3. Торгівельні марки (знаки для товарів та послуг): використовується для захисту слоганів, символів і логотипів, які застосовуються для опису або ідентифікації продукту або послуги, а також захищають їх до тих пір, поки знак перебуває у використанні.

4. Комерційні таємниці: використовуються для захисту процесів, методів і формул, які повинні зберігатися в таємниці, щоб надати підприємству конкурентну перевагу (наприклад, секретна формула напою "Кока-Кола"). Найбільш важливим поняттям для цього типу інтелектуальної власності є те, що вона містить таємницю.

Загрози для системи інтелектуальної безпеки можуть виникати як ззовні так і зсередини самого підприємства. Зсередини підприємства загрози можуть формуватися зі сторони самих працівників підприємства, діяльність яких направлена на зниження перспектив використання інтелектуального потенціалу підприємства. З зовні загрози можуть формуватися зі сторони фірм-конкурентів, впливи яких мають на меті переманювання кваліфікованого персоналу, котрий має вагомий інтелектуальний потенціал та володіє даними про інтелектуальну власність підприємства (економічна розвідка або ж промислове шпигунство).

Водночас загрозами для інтелектуальної безпеки підприємства можуть бути недооцінка важливості праці залучених ззовні професіоналів, громад, заниження їх ролі для діяльності підприємства. Як уже зазначалося в попередніх дослідженнях автора, у деяких випадках ці іноземні компанії, які видають себе за приватні охоронні фірми, насправді виступають в ролі промислових «розвідників», що проводять моніторинг незахищених об'єктів права інтелектуальної власності на території України, співпрацюючи з вітчизняними конкурентами в своїй країні [3, с. 159].

Підприємства, зокрема, володіють значною кількістю інтелектуальної власності, що вимагає відповідного рівня охорони та захисту. Працівники працюють над НДДКР, розробляють науково-дослідні програми, які своїм результатом мають створення винаходів, та водночас є науковими працями, що володіють високим рівнем потенціалу, що потенційно може приносити користь суспільству. Для того, щоб захистити основні результати, керівник може використовувати систему інтелектуальної безпеки на всіх етапах інноваційного процесу: відкриття, оцінка та виконання:

1. Відкриття: на стадії відкриття загальні інформаційні концепції інтелектуальної безпеки, такі як контроль доступу, управління активами, криптографія мають важливе значення для забезпечення того, щоб тільки працівники, що безпосередньо беруть участь у даному процесі, мали доступ до розробок, дизайну і техніко-економічного обґрунтування інформації. Основна концепція інтелектуальної безпеки – це конфіденційність.

2. Оцінка: використання оперативного контролю інтелектуальної безпеки може забезпечити надійність методологій проектування і результати випробувань. Основна концепція інтелектуальної безпеки на цій стадії – це цілісність.

3. Виконання: коли винахід готовий до випуску і комерціалізації, використання механізмів контролю інтелектуальної безпеки може гарантувати, що будь-які ІТ-ресурси або дані, необхідні відповідно для випуску винаходу, можуть бути доступними та надійними. Основна концепція інтелектуальної безпеки даної стадії – це доступності.

Усе вищезазначене дозволяє зробити висновок, що побудова системи інтелектуальної безпеки на підприємстві є необхідною умовою його подальшого результативного функціонування, що вимагає вирішення чисельних завдань правового та економічного характеру щодо захисту своїх інтересів в контексті охорони та захисту об'єктів інтелектуальної власності підприємства.

Етапи побудови системи інтелектуальної безпеки підприємства, на думку автора, повинні включати в себе:

1. Дослідження специфіки сфери діяльності підприємства, сегментів ринку, його конкурентоспроможності.

2. Оцінку зовнішніх та внутрішніх загроз для системи інтелектуальної безпеки підприємства.

3. Дослідження даних про перспективу виникнення кризових ситуацій на ринку та проектування можливої поведінки підприємства в них.

4. Аудит існуючих об'єктів інтелектуальної власності на підприємстві та аналіз їх рівня охорони.

5. Моделювання сучасної системи інтелектуальної безпеки на підприємстві: формування плану дій з усунення виявлених під час перевірки недоліків; формування пропозицій по удосконаленню існуючої системи інтелектуальної безпеки, розрахунок усіх видів необхідних ресурсів; складання кошторису витрат на забезпечення відповідного рівня функціонування системи інтелектуальної безпеки на підприємстві, складання бюджету.

6. Контроль за функціонуванням створеної системи інтелектуальної безпеки.

7. Оцінка ефективності роботи системи інтелектуальної безпеки на підприємстві.

8. Коректування та удосконалення системи інтелектуальної безпеки (у випадку необхідності).

Отже, головною метою побудови системи інтелектуальної безпеки на підприємстві є: запобігання та протидія зовнішнім та внутрішнім загрозам підприємства; забезпечення стабільного розвитку підприємства; запобігання втрати нематеріальних ресурсів; захист від протиправних посягань на інтелектуальні ресурси; забезпечення ефективної діяльності всіх підрозділів підприємства.

ЛІТЕРАТУРА*:*

1. Брукинг З. Интеллектуальный капитал: [Пер. с англ.] / З. Брукинг. – СПб: Питер, 2001. – 288 с.

2. Мосов С.П. Інтелектуальна безпека України в контексті її входження до СОТ / С.П. Мосов, А.Г. Жарінова // Інтелектуальна власність. – 2008. – №6. – С. 4-9.

3. Якубівська Ю. Є. Вплив промислового шпигунства на сферу інтелектуальної власності / Ю. Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право: Науковий журнал. – К. : УДУФМТ, 2013. – № 4 (69). – С. 158-162.