УДК 658.15.012.8

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Х. В. Сігова, *студ. гр.МЕ-14*[6]
Кіровоградський національний технічний університет

Особливість сучасної світової економіки полягає у стійкій тенденції прискорення темпів економічного та науково-технічного розвитку. В той же час зростають ризики господарської діяльності, рівень ймовірних загроз, як для життя окремої особистості, так і для діяльності підприємств та установ. У цій ситуації правова, економічна, політична і соціальна інформація, як чинник забезпечення безпеки, набуває все більшого значення [1, с. 220].

У наукових працях вітчизняних та зарубіжних вчених-економістів представлено численні дослідження інформаційної безпеки підприємства. Однак актуальні питання забезпечення інформаційної безпеки підприємства залишаються все ще маловивченими.

Різні аспекти інформаційної безпеки підприємства, досліджувалися багатьма вітчизняними і зарубіжними вченими. Серед них варто відзначити таких, як: В. Геєць, Р. Руденський, Л. Абалкін, В. Ігнатьєв, Ю. Лисенко, А. Спірідонов, В. Щербина.

Незважаючи на істотну кількість наукових праць, присвячених питанням даної проблематики, слід констатувати відсутність комплексного дослідження системи забезпечення національної економічної безпеки в контексті залучення країни до процесів економічної інтеграції на сучасному етапі розвитку глобального світового господарства.

Дослідження основних аспектів забезпечення інформаційної безпеки підприємства полягає у дослідженні теоретичних положень щодо оцінки та забезпечення інформаційної безпеки підприємства, зокрема суб'єктів інформаційного середовища та запобігання негативного інформаційного впливу на них.

У практичному плані інформаційна безпека існує лише у взаємозв'язку із суб'єктом інформаційного середовища, саме суб'єкт диктує показники такої безпеки. Це стосується не тільки конкретних суб'єктів, але і до особистості, суспільства та держави.

Інформаційна безпека суб'єкта не може бути забезпечена без наявності у нього необхідної інформації. Інформаційні потреби різних суб'єктів не однакові, але для будь-якого суб'єкта відсутність можливості отримання необхідної інформації може мати негативні наслідки. Ці наслідки можуть носити різний характер, їх важкість залежить від складу відсутньої інформації.

Необхідна для задоволення інформаційних потреб інформація повинна відповідати певним вимогам:

1) інформація повинна бути відносно повною, оскільки абсолютно повної інформації жоден суб'єкт мати не може. Повнота інформації характеризується її достатністю для прийняття правильних рішень;

2) інформація повинна бути достовірною, бо недостовірна інформація призводить до прийняття неправильних рішень;

3) інформація повинна бути своєчасною, оскільки необхідні рішення ефективні лише тоді, коли вони приймаються вчасно [2, с. 13]. Прийняттю неправильних рішень може сприяти наявність шкідливої, небезпечної для суб'єкта інформації, яка найчастіше цілеспрямовано нав'язується.

Це вимагає забезпечення захисту суб'єктів інформаційних відносин від негативного інформаційного впливу, що є ще однією складовою інформаційної безпеки.

[6] Науковий керівник – О. В. Заярнюк, к.е.н., доцент Кіровоградського національного технічного університету

У Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.» цей термін набуває такого трактування: «інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [4].

При забезпеченні інформаційної безпеки важливо враховувати ті завдання, які висуваються перед сторонами, зацікавленими в інформаційній безпеці, а саме:

1) забезпечення доступності інформації, що має на увазі можливість за прийнятний час отримати необхідну інформаційну послугу, а також запобігти несанкціонованій відмові в отриманні інформації;

2) забезпечення цілісності інформації, що передбачає запобігання несанкціонованої модифікації або руйнування інформації;

3) забезпечення конфіденційності інформації, що пов’язано із запобіганням несанкціонованого ознайомлення з інформацією.

Належні служби підприємства виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової безпеки підприємства. До таких належать:

- збирання всіх видів інформації, що має відношення до діяльності того чи іншого суб’єкта господарювання;
- аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів і методів;
- прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів;
- оцінка рівня економічної безпеки за всіма складовими та в цілому, розробка рекомендацій для підвищення цього рівня на конкретному суб’єкті господарювання;
- інші види діяльності з розробки інформаційної складової економічної безпеки.

На підприємство постійно надходять потоки інформації, що розрізняються за джерелами їхнього формування. Заведено відокремлювати:

- відкриту офіційну інформацію;
- вірогідну нетаємну інформацію, одержану через неформальні контакти працівників фірми з носіями такої інформації;
- вірогідну нетаємну інформацію, одержану через неформальні контакти працівників фірми з носіями такої інформації.

Серед існуючих засобів забезпечення безпеки підприємства можна виокремити наступні:

1) Технічні засоби. До них відносяться охоронно-пожежні системи, відео-радіоапаратура, засоби виявлення вибухових приладів, бронежилети, огородження тощо.

2) Організаційні засоби. Створення спеціалізованих оргструктурних формувань, що забезпечують безпеку підприємства.

3) Інформаційні засоби. Передусім це друкована і відеопродукція з питань збереження конфіденційної інформації. Крім цього, важлива інформація для прийняття рішень з питань економічної безпеки зберігається на комп'ютерах.

4) Фінансові засоби. Без достатніх фінансових коштів не можливе функціонування системи економічної безпеки підприємства, питання лиш в тому, щоб використати їх цілеспрямовано та з високою віддачею.

5) Правові засоби. Підприємство повинне у своїй діяльності керуватися не лише виданими вищестоящими органами влади законами та підзаконними актами, але й розробляти власні локальні правові акти з питань забезпечення економічної безпеки підприємства.

6) Кадрові засоби. Підприємство повинне бути забезпечене кадрами, що займаються питаннями економічної безпеки.

7) Інтелектуальні засоби. Залучення до роботи кваліфікованих спеціалістів, наукових робітників, що дозволяє модернізувати систему безпеки підприємства.

Одночасне впровадження усіх цих засобів неможливе. Воно проходить у кілька етапів:

I етап. Виділення фінансових коштів.

II етап. Формування кадрових і організаційних засобів.

III етап. Розробка системи правових засобів.

IV етап. Залучення технічних, інформаційних та інтелектуальних засобів.

Переведені з статичного в динамічний стан вищевказані засоби перетворюються в методи забезпечення економічної безпеки підприємства. Відповідно можна виділити технічні, інформаційні, фінансові, правові, інтелектуальні методи. Наведемо стислий перелік цих методів

1. Технічні – спостереження, контроль, ідентифікація;

2. Інформаційні – складання характеристик на працівників, аналітичні матеріали конфіденційного характеру тощо;

3. Фінансові – матеріальне стимулювання працівників, що мають досягнення в забезпеченні економічної безпеки підприємства;

4. Правові – судовий захист законних прав і інтересів, сприяння діям правоохоронних органів;

5. Кадрові – підбір, навчання кадрів, що забезпечують безпеку підприємства;

6. Інтелектуальні – патентування, ноу-хау тощо.

Інформаційна безпека має одне з першочергових значень для соціально-економічного розвитку держави. Україна має продовжити активні кроки на шляху розбудови власної системи інформаційної безпеки. Важливими заходами в цьому процесі мають стати організація і проведення інформаційних операцій, а також розвиток системи сертифікації інформаційних продуктів. Окрім того, система забезпечення інформаційної безпеки повинна гнучко коригуватися відповідно до мінливого характеру зовнішніх та внутрішніх факторів оточення [3, с. 15–17].

Список літератури

1. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ / В. М. Щербина // Актуальні проблеми економіки. – 2006. – № 10. – С. 220–225
2. Информационная безопасность государственных организаций и коммерческих фирм: справочное пособие / под общ. ред. Л. Д. Реймана. – М.: НТЦ ФИОРД–ИНФО, 2002. – 272 с.
3. Игнатьев В. А. Информационная безопасность современного коммерческого предприятия: монография / В. А. Игнатьев. – Старый Оскол : ООО «ТНТ», 2005. – 448 с.
4. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/537–16