

Електронне наукове фахове видання "Ефективна економіка" включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)

Ефективна ЕКОНОМІКА

Дніпропетровський державний аграрно-економічний університет



№ 6, 2013 [Назад](#) [Головна](#)

УДК 65.012.8

*Н. О. Бабіна,
старший викладач кафедри економіки факультету ринкових, інформаційних та інноваційних технологій
Київський національний університет технологій та дизайну, м. Черкаси*

ГЛОБАЛІЗАЦІЙНІ ТРАНСФОРМАЦІЇ ТА ЕКОНОМІЧНА БЕЗПЕКА

*N. O. Babina,
Sr. Instructor of Economics Department, Kyiv National University of Technologies and Design, School of Market, Information and Innovative Technologies at Cherkassy*

GLOBALIZATION TRANSFORMATIONS AND ECONOMIC SECURITY

Висвітлені основні проблеми економічної безпеки вітчизняних суб'єктів господарювання в умовах глобалізаційних трансформацій. Запропоновано класифікацію небезпек за рівнем збитку, який несе загроза, якщо її не відвернути, що має практичну цінність при акомодатії рівня економічної безпеки підприємств до модернових умов функціонування в глобальному середовищі.

The key issues in economic security of national economic entities in the situation of globalization transformations are highlighted. The taxonomy of threats in terms of their not averted losses is offered. It has its practical value when accommodating the level of economic security at enterprises in modern situation of their performance in global environment.

Ключові слова: глобалізація, трансформаційні процеси, економічна безпека, загрози, інформаційна безпека підприємства.

Keywords: globalization, transformation processes, economic security, threats, information security of enterprise.

Постановка проблеми. В умовах глобалізації комплекс соціально-економічних, політичних та правових факторів різко загострив проблему формування та забезпечення безпеки конститутивних компонентів ієрархічної економічної системи трансформаційної економіки України. Найважливішою складовою частиною національної безпеки країни є економічна безпека, оскільки вона нерозривно зв'язана з економічною ефективністю функціонування суб'єктів господарської діяльності та з процесом розвитку суспільства в цілому.

Аналіз останніх досліджень і публікацій. Сучасні закордонні розвідки в більшій мірі націлені на дослідження, перш за все, економічної безпеки на мега-рівні. Так, економічна безпека країни тлумачиться як комплексна багатофакторна категорія, що описує здатність національної економіки до стійкого розвитку з метою задоволення потреб суспільства і держави, відповіді на загрози для національної безпеки і задоволення національних інтересів, підтримку конкурентоспроможності національної економіки в світовому економічному просторі (Б.Лопес, К.Савка). Особливе місце займають дослідження безпеки під кутом зору глобалізаційних тенденцій. Так, в полі зору учених опиняються джерела новітніх загроз і референтів безпеки (Е. Колодзей, А.Тікнер, Д.Болдуїн, Б.Бьюзан); екологічні (Д.Фьерке), соціальні (Д.Голдфішер), мікроекономічні (Д.Флігстейн) правові (К.Краузе, М.Вільямс), інституціональні (Лью та Ф.Сото), особистісні (С.Волт, М.Лаффер) аспекти економічної безпеки; чільне місце займають питання інформаційної безпеки (Л. Дж. Хоффман, Ф.Гансен).

Проблема економічної безпеки отримує суттєвий розвиток в Україні з середини 90-х років, коли молода держава і вітчизняні підприємства стикаються з необхідністю урахування ризиків в перехідній економіці; потребою своєчасної адекватної реакції на зміни з метою забезпечення адаптації всіх елементів системи до новітніх умов функціонування.

Серед сучасних напрямів наукових розвідок вітчизняних вчених у сфері економічної безпеки провідними є: різні аспекти управління розвитком підприємства в новій економіці (І. Ансоф, А.Н. Богатко, Б.Л. Кучін, О.І. Пушкар, О.М. Тридід, Є.В. Якушева); оцінка рівня економічної безпеки в умовах невизначеності та ризику (О.В. Ареф'єва, Г.А. Андрощук, М.М. Єрмошенко, Т.С. Клебанова, Г.Б. Козаченко, А.В. Крисін, Т.Б. Кузенко, В.І. Мунтян, Є.А. Олейніков, В.С. Пономаренко, В.Л. Тамбовцев, О.І. Черняк, М.Я. Швець); стратегії та механізми забезпечення економічної безпеки в контексті інтеграційних процесів (В.Г. Алькема, О.Г. Білорус, Т.Г. Васильців, В.І. Волошин, Д.Г. Лук'яненко, О.А. Кириченко). Проте деякі важливі аспекти економічної безпеки потребують більш детального дослідження. Насамперед, це стосується взаємозв'язку економічної безпеки (підприємства, зокрема) та глобалізаційних трансформацій.

Основна мета дослідження – показати, які аспекти проблеми економічної безпеки актуалізуються в умовах системних трансформацій в Україні і визначити певні практичні заходи їх вирішення на рівні функціонування корпоративного сектору (підприємств), зокрема.

Виклад основного матеріалу. Глобалізація соціально-економічних процесів супроводжується, з одного боку, формуванням новітніх умов і джерел розвитку, а з іншого — несе в собі виклики: технологічні, економічні, соціальні, цивілізаційні, які актуалізують питання безпеки. Найбільш актуальною проблемою економічної безпеки є для країн, які знаходяться у процесі системних трансформацій. Провідною суперечністю для них є, з одного боку, необхідність інтеграції у світогосподарську структуру, а з іншого - потреба забезпечення певної захищеності від наслідків ймовірних криз цих структур.

В таких умовах питання економічної безпеки підприємства є значущим як на державному, регіональному, так і на рівні окремих господарюючих суб'єктів, оскільки сучасні наслідки економічної глобалізації (що може мати як позитивний ефект для забезпечення економічної безпеки у вигляді різних технічних відкриттів та розробок, так і негативний – у формі експлуатації одних держав іншими) є викликом не тільки державі, але і підприємствам.

Функціонування у глобальному конкурентному середовищі з необхідністю стимулює пошук принципово нових підходів до забезпечення економічної безпеки вітчизняних підприємств на зовнішніх ринках та зміцнення потенціалу їх розвитку. Підґрунтям підвищення рівня економічної безпеки суб'єктів господарської діяльності є формування та розвиток модерної системи економічної безпеки, що підвищує значення ідентифікації компонентів та специфіки функціонування підсистеми нижчих рівнів, їх взаємозв'язків і взаємовпливів; узгодження інтересів кожної підсистеми з економічними інтересами всієї системи.

Економічна безпека підприємства розуміється нами як такий стан його функціонування, за якого забезпечується неодмінний розвиток у відповідності до задалегідь визначених (задекларованих) цілей і завдань; спроможність зберігати стійкість до внутрішніх та зовнішніх загроз; здатність задовольняти потреби зацікавлених агентів. Натомість в умовах фінансово-економічної кризи українського підприємства зазначали значних втрат, пов'язаних із стрімким падінням попиту, відтоком капіталу, подорожчанням кредитного ресурсу, нестабільністю макроекономічного середовища.

Основними чинниками, що здійснюють найбільш негативний вплив на формування рівня економічної безпеки, є: висока енергетична залежність країни, відсутність міжнародних гарантій щодо постачання стратегічної сировини і енергоресурсів на довгостроковій основі; позаекономічний підхід до формування ціни на енергоносії по відношенню до України; технологічна відсталість промисловості, що ставить Україну на рівень з країнами третього світу за рівнем

конкурентоспроможності; фінансова залежність вітчизняної економіки від інших країн і міжнародних фінансових організацій; діяльність тінювих структур, неконтрольований відтік за межі України інтелектуальних, матеріальних і фінансових ресурсів; глибока взаємна дифузія капіталу і влади, неефективний розподіл та відсутність дієвого контролю за використанням бюджетних коштів; неефективний розподіл власності, і, як наслідок, дискримінаційний розподіл доходів в економіці, що призводить до подальшої поляризації суспільства, зниження рівня життя населення.

В умовах посткризового зростання, в якому нині перебуває економіка України, виникають нові виклики та ризики підтримки стабільного розвитку підприємств, які актуалізують проблему їх економічної безпеки. Серед цих ризиків: загострення конкуренції за доступ до економічних ресурсів (сировинних, фінансових, інтелектуальних), штучне обмеження можливостей щодо виходу на фінансові ринки, відновлення проблеми рейдерства (переходу права власності з використанням корупційних схем) тощо.

Для досягнення необхідного рівня економічної безпеки сучасним українським підприємствам належить вирішити низку проблем, серед яких визначальними є: створення системи превентивних заходів щодо уникнення впливу зовнішніх і внутрішніх загроз; підвищення якості інформації щодо конкурентів і власної діяльності, яка складає основу визначення цілей і стратегії підприємства; аналіз витрат на економічну безпеку і включення його до кошторису підприємства; актуалізація наявних можливостей підприємства та спрямування системи економічної безпеки на попередження загроз чи нейтралізацію їх негативних впливів.

В умовах посткризового зростання значно загострюються ризики у сфері підтримки інформаційної безпеки підприємства. Сьогодні, коли підприємство самотужки формує та реалізує задачі забезпечення власної інформаційної безпеки, а недобросовісні конкуренти усе частіше активно шпигують за економічно значущою інформацією, варто пам'ятати, що інформаційна безпека є одним з ключових показників вдалої діяльності господарюючих суб'єктів.

Для успішного функціонування системи інформаційної безпеки підприємства, перш за все, необхідно визначити коло найбільш вірогідних загроз (чинників, що їх спричиняють) для суб'єкта господарювання і оцінити рівень їх актуалізації; виявити найбільш вразливі місця в інформаційній системі, постійно їх моніторити; розробити систему заходів профілактики та мінімізації збитків (наслідків реалізації загроз), що спричинені інформаційним продуктам, ресурсам, інформаційній інфраструктурі суб'єкта в цілому.

Особливо підкреслимо, що при створенні системи інформаційної безпеки підприємство має врахувати свої специфічні особливості інформаційної взаємодії з іншими суб'єктами ринку, серед яких провідне місце займають: конкурентоздатність продукції на внутрішніх і зовнішніх ринках; інноваційний рівень техніки і технологій; практика спілкування з контрагентами на основі Internet-технологій; укладання угод та реалізація продукції за допомогою використання E-commerce тощо.

Інформаційні об'єкти безпосередньо або опосередковано знаходяться під прицілом загроз, що виходять від суб'єктів – джерел загроз і є результатом модифікації інформаційного поля чи зв'язані з недоліками власної системи інформаційної безпеки. Можливість виникнення і реалізації загроз мобілізує суб'єктів, що забезпечують інформаційну безпеку, стимулює їх вирізнити можливих ризиків, прорахувувати ймовірні збитки та їх величини.

Об'єктами загроз, до яких застосовуються інформаційні технології з метою нанесення збитку, сьогодні стають: інформаційні процеси, інформаційні продукти, персонал, що долучається до інформації, інформаційна інфраструктура в цілому, найбільш вразливими в якій є: процеси, пов'язані з обробкою інформації; архітектури мереж передачі і обробки інформації; засоби комп'ютерної техніки, що використовуються для обробки; різні види забезпечення, які супроводжують процеси введення, обробки й аналізу даних; комунікації, що забезпечують інформаційну взаємодію із зовнішнім середовищем підприємства. Атаці можуть бути піддані блоки управління доступом до конфіденційної інформації, система блокування незаконного вторгнення та ін.

Саме цінна, конфіденційна інформація, що відноситься до комерційної таємниці та окреслюється тим реальним прибутком, який можна одержати від її використання, становить особливий інтерес для підприємницького шпигунства. З метою нанесення збитку конкуренти все частіше застосовують новітні інформаційні технології, яким важко протистояти. Тому, на наш погляд, плідно з практичної точки зору може виявитися систематизація інформаційних загроз за рівнем збитку, який несе загроза, якщо її не відвернути.

Таблиця 1. Класифікація інформаційних загроз

Загроза	Превентивні заходи
	Згубний (фатальний) рівень збитку
Невірне визначення та оцінка рівня інформаційної безпеки	Розробка комплексної програми безпеки, що містить норми і правила, регламентує політику і практику інформаційної безпеки тощо.
Збої у програмному (системному та прикладному) забезпеченні	Установлення ліцензійного програмного забезпечення.
	Відчутний (сильний) рівень збитку
Висока ймовірність розголошення комерційної таємниці	Розробка документів, що регламентують рівень доступу посадових осіб до інформації, що включає таємницю.
Нецільове використання інформаційних ресурсів	Розробка посадових інструкцій, що обмежують доступ до інформації, інформаційних продуктів і програмно-апаратних засобів.
Витік інформації	Установлення профілів захисту у відповідності до стандарту ISO/IEC 15408) Постійний контроль за передачею інформації по всім основним вузлам каналів зв'язку: блокування можливості несанкціонованого доступу до інформації, можливості обробки і передачі її та інформаційних продуктів (у тому числі з віддалених терміналів у комп'ютерних мережах); збереження цілісності та конфіденційності інформації; недопущення модифікації авторизованої інформації.
Несанкціонована модифікація інформаційної системи програмними вірусами, логічними закладками, програмами на кшталт Троянського коня.	Блокування незаконної модифікації системного та прикладного програмного забезпечення протягом усього життєвого циклу інформаційної системи а допомогою спеціальних програм
Брак обов'язкової процедури тестування програмного забезпечення	Правильна організація експлуатації наявного програмного забезпечення.
	Середній (помірний) рівень збитку
Незбалансованість системи управління інформаційними ресурсами	Визначення процедур і механізму реалізації адміністративного контролю за програмно-апаратними засобами.
Фіксація несанкціонованих входів в інформаційну систему	Запровадження процедури ідентифікації користувачів.
Порушення якісних властивостей профілів захисту	Встановлення процедур адміністрування паролів
Неефективні управлінські рішення, невдалі угоди на основі недостовірної інформації	Використання тільки перевірених джерел інформації
	Невеликий (слабкий) рівень збитку
Відкритий доступ до авторизованої інформації	Запровадження процедур аутентифікації та процедур захисту файлів
Збільшення обсягів інформації (збільшення зайвої, непотрібної інформації - інформаційний шум)	Блокування за допомогою спеціальних засобів і програм надлишкової, непотрібної і несвоєчасної інформації; оволодіння аналітиками, що працюють з інформацією, основними принципами захисту від маніпулятивних впливів.

Складено особисто автором

Дана класифікація може бути корисною при аналізі загроз інформаційній безпеці, розробці адекватних заходів забезпечення та підтримки інформаційної безпеки, реалізації запланованих дій, а також при побудові моделі інформаційної безпеки підприємницької діяльності промислового підприємства.

Висновки. Сучасні тенденції функціонування глобальних економічних систем підтверджують, що економічна безпека як економічне явище в існуючих умовах набуває важливого значення для забезпечення ефективного функціонування усіх господарюючих суб'єктів на міжнародній арені.

Сучасне підприємство, яке функціонує у невизначеному економічному середовищі, змушено в постійній боротьбі з конкурентами приймати ризиковані

рішення, попереджати, послаблювати та захищатися від актуальних та латентних небезпек і загроз (в площині залучення інвестицій, фінансів, кваліфікованого персоналу; поставок товарно-матеріальних цінностей; придбанні новітніх технологій; обміну інформацією тощо), використовуючи увесь спектр корпоративних ресурсів за для досягнення своєї головної мети - забезпечення інтенсивного розвитку, своєї економічної незалежності.

Інформація в сучасних умовах господарювання виступає важливим чинником виробництва, а інформаційна безпека – конститутивною частиною системи корпоративної економічної безпеки підприємства.

Класифікація небезпек за рівнем збитку, який несе загроза, якщо її не відвернути, має практичну цінність при акомодатії рівня економічної безпеки вітчизняних підприємств до модернових умов функціонування в глобальному середовищі.

Список використаних джерел

1. Дубницький В. И. Эволюция, сущность, классы, инструментарий электронного бизнеса: [монография] / Дубницький В. И., Лазикова А. И. / НАН Украины, Ин-т экономики промышленности, Донец. экономико-гуманитарный ин-т. - Донецк: Юго-Восток, 2004. - 84 с.
2. Козаченко А.В. Економічна безпека підприємства: сутність та механізм забезпечення: монографія / А.В. Козаченко, В.П. Пономарьов, О.М. Ляшенко. – К.: Лібра, 2003. – 280 с.
3. Прокоф'єва Д. М. Підприємницьке шпигунство в системі інформаційних злочинів // Український центр інформаційної безпеки / www.bezpeka.com/library/lib_aspect.html.
4. Bernardo V. Lopez. Upshot; Business intelligence: the Japanese model. // Business World, 17 июня 1999, с. 4 (на англ. яз.).
5. Kenneth Sawka, вице-президент компании Fuld & Company Inc. The analyst's corner: It's good be needed //Competitive Intelligence Magazine, Vol. 4, No. 2; 2001.

Стаття надійшла до редакції 19.06.2013 р.



ТОВ "ДКС Центр"