

ІНФОРМАЦІЙНИЙ СКЛАДНИК ЕКОНОМІЧНОЇ БЕЗПЕКИ ГАЛУЗІ

ECONOMIC COMPONENT OF THE ECONOMIC SECURITY OF THE INDUSTRY

Денисов О.Є.

докторант,
Університет економіки та права «КРОК» (м. Київ)

У статті досліджено підходи до визначення інформаційної безпеки галузі. Особлива увага приділяється питанню класифікації загроз інформаційній безпеці. Автором підкреслюється важливість розуміння загроз та небезпек, що можуть впливати на економічну безпеку галузі. Розглядається класифікація цих загроз, а також завдання інформаційної безпеки галузі.

Ключові слова: інформаційна безпека, економічна безпека, галузь, загрози, внутрішній ринок, міжнародний ринок, управлінські рішення, інформація, управління інформацією, обробка інформації.

В статье исследованы подходы к определению информационной безопасности отрасли. Особое внимание уделяется вопросу классификации угроз информационной безопасности. Автором подчеркивается важность понимания угроз и опасностей, которые могут влиять на экономическую безопасность отрасли. Рассматривается классификация этих угроз, а также задачи информационной безопасности отрасли.

Ключевые слова: информационная безопасность, экономическая безопасность, отрасль, угрозы, внутренний рынок, международный рынок, управленческие решения, информация, управление информацией, обработка информации.

This article aims to examine existing approaches to determining the information security of the industry. The article focuses on the issue of threats to information security classification. The author emphasizes the importance of understanding the threats and dangers associated with the information security of the industry, which can affect the economic security of the industry. Along with that, the classification of these threats is considered. The range of information security tasks in the industry is also described.

Keywords: information security, economic security, industry, threats, domestic market, international market, management decisions, information, information management, information processing.

Постановка проблеми. У загальному контексті інформація – це відомості про осіб, явища, події, предмети, факти, процеси, що мали місце в будь-якій сфері життєдіяльності суспільства.

Інформація та інформаційна безпека галузі є проміжним невидимим полем, мембраною між галуззю країни, її підприємствами та зовнішнім економічним і внутрішнім економічним ринком. Внутрішня інформація галузі про стан внутрішніх ресурсів є інформацією, яка задовольняє потреби в матеріальних, технологічних, кадрових та інших ресурсах та через продаж продукції на внутрішньому ринку стимулює збут основної маси продукції і надходження фінансових ресурсів. Зовнішнє поле є стимулом для розвитку, розкриваючи нові горизонти та можливості інтеграції на зовнішньоекономічні ринки. Зовнішнє поле несе в собі репрезентативне навантаження, оскільки має проінформувати світову економічну спільноту про можливості та пропозиції, які надає галузь у світовій ринковій співпраці.

Сутність та фактори дії інформаційного складника економічної безпеки галузі досить

повно описує поняття асиметричної інформації. Так, існує наукова парадигма, згідно з якою під асиметричною інформацією розуміють ситуацію, у якій частина учасників угоди володіє вичерпною та точною інформацією, тоді як інші учасники нею не володіють, оскільки обидві сторони інформаційного обміну (галузь та зовнішньоекономічна міжнародна спільнота, галузь та контрагенти внутрішнього ринку) володіють інформацією про одні й ті самі об'єкти чи процеси різною мірою та в різному обсязі [1]. Наявність асиметричної інформації приводить до того, що дві сторони угоди не завжди мають вільний доступ до вичерпної та повної інформації для прийняття управлінського рішення, що приводить до неефективності їх ринкової співпраці.

Відповідно до цього завданням інформаційного складника економічної безпеки галузі є таке формування зовнішнього економічного поля своєї діяльності, яке б максимально повно та позитивно інформувало міжнародну спільноту про галузь, їх структуру, пропозиції, переваги, особливості державного регулювання у межах міжнародної співпраці, науку, культуру,

традиції та інші фактори, що могли би стати для міжнародного ринку сферами реалізації економічних інтересів і сприяли б залученню вітчизняних галузей до процесу міжнародного торгового, технологічного та культурного співробітництва. Реалізація таких завдань можлива через активне просування позитивної інформації про країну в Інтернеті та міжнародних ЗМІ, участь країни та представників бізнесу (галузей) у міжнародних форумах, конференціях, виставках та інших наукових, економічних, суспільно-політичних заходах міжнародного рівня, активну участь держави та державних органів та інституцій у подіях та процесах міжнародного суспільно-економічного та культурного життя. Всі ці процеси пов'язані зі створенням, формуванням, передачею та отриманням позитивної релевантної інформації про країну та її економіку загалом і про галузі та підприємства, що формують її економічну структуру та представляють її національні економічні інтереси на міжнародній арені. Інформаційні поля в зовнішньоекономічній та внутрішньоекономічній діяльності галузі представлені на рис. 1.

Водночас галузі мають формувати внутрішнє поле економічної безпеки, яке полягає в активному інформаційно-аналітичному обміні із постачальниками, конкурентами, підрядниками, державними контролюючими та регулюючими органами, суспільними та громадськими організаціями, ЗМІ та іншими організаціями; формувати інформаційні комунікації з потенційними споживачами продукції галузі, оскільки обсяг внутрішнього ринку формується саме спільнотою всіх наявних та потенційних покупців та обсягом спожитих товарів і благ.

Аналіз останніх досліджень і публікацій.

Інформаційна безпека та формування механізму інформаційно-аналітичного забезпечення як складника економічної безпеки невід'ємно

пов'язані із процесом управління інформацією, що досліджувалося у працях багатьох провідних науковців.

Так, на думку Е. Мейсона та В. Стайбіка, управління інформацією – це процес планування, організації, підбору кадрів, управління, координації різних видів інформаційної діяльності та контролю за ними, включаючи означення інформаційних послуг, систем і форматів, із метою досягнення цілей організації [5]. За визначення П. Шолтіса, управління інформацією – це метод організації інформації та інформаційної технології з метою задоволення потреб організації через оптимізацію використання інформації, мінімізацію витрат і чіткий розподіл обов'язків [6]. Г. Верзіг визначив процес управління інформацією як інтеграцію комунікацій, яка має три аспекти: управління комунікаціями, управління інформаційними ресурсами та управління обробкою інформації [7]. На думку М. Атінджера, управління інформацією – це інтегрована інформаційна структура, балансування всіх складників якої забезпечується інформацією [8].

Л.М. Калініна визначає управління інформацією як складний, багатогранний і нелінійний процес суб'єкт-суб'єктної, суб'єкт-об'єктної, об'єкт-об'єктної інформаційно-комунікаційної взаємодії та взаємозв'язку в просторі та в часі на основі ІР, який спрямований на організацію, проектування і координацію програм, заходів задля досягнення визначеної мети функціонування та розвитку [9]. Основою управління інформацією за Є. Фогелем є інформаційні ресурси, основним призначенням яких є координація обробки інформації [8]. Інформаційний складник у забезпеченні економічної безпеки підприємства визначається як комплекс програмного, обчислювально-технічного та організаційного забезпечення, а також обчислювального персоналу, призначений для забез-

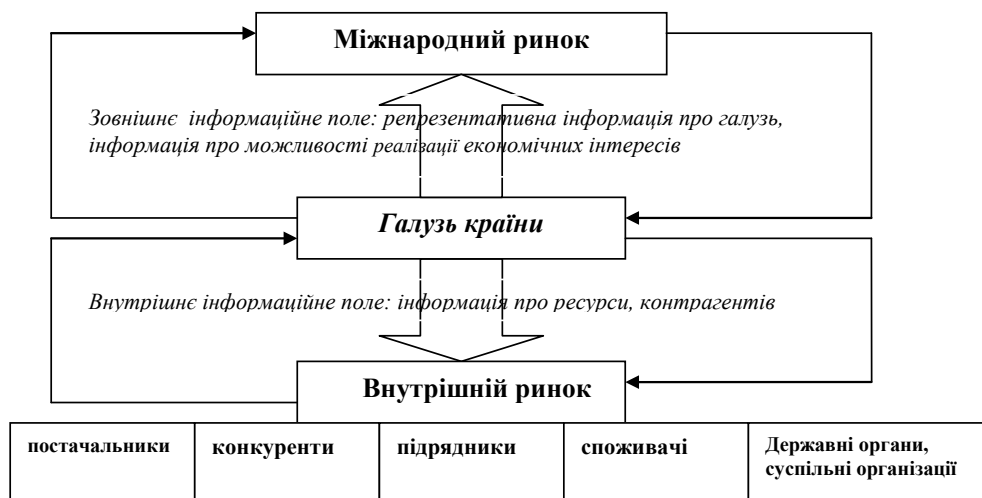


Рис. 1. Інформаційні поля у зовнішній та внутрішній економічній діяльності галузі

Джерело: розроблено автором на основі [2; 3; 4; 5]

печення користувачів необхідною інформацією в конкретній галузі діяльності [10].

Загалом інформаційна безпека – це захищеність інформаційних систем і інформаційних ресурсів від зовнішніх та внутрішніх загроз, що ускладнюють ефективно використання інформації суспільством, державою, окремими індивідуумами [1]. Місце інформації та інформаційно-аналітичного забезпечення у функціонуванні структурних утворень на всіх рівнях економіки, починаючи від підприємства, галузі як сукупності підприємств, держави та світового суспільного простору, постійно зростає та із процесами інтеграції і глобалізації набуває нових масштабів та нового домінантного значення.

Отже, узагальнюючи досліджений матеріал, можна сформулювати загальне визначення, згідно з яким інформаційна безпека галузі – це такий стан формування та розвитку інформаційно-аналітичного забезпечення галузі, який дає змогу ефективно презентувати галузь на зовнішньоекономічних ринках та забезпечити високий рівень інформаційно-аналітичного забезпечення і безпеку на внутрішньому ринку країни та в діяльності кожного окремого підприємства як невід’ємного складника галузі.

Під час розгляду інформаційної безпеки галузі недостатньо уваги приділено її впливу на економічну безпеку галузі.

Метою статті є визначення загроз та небезпек, пов’язаних з інформаційною безпекою галузі, що можуть впливати на економічну безпеку галузі, класифікація цих загроз та формування завдань інформаційної безпеки галузі.

Виклад основного матеріалу дослідження. Інформаційна безпека галузі – це стан забезпечення підприємств галузі інформаційними ресурсами та підвищення ефективності збору, обробки та використання інформації зовнішнього та внутрішнього конкурентного середовища галузі з метою підвищення рівня інформаційно-аналітичного забезпечення галузі та підприємств, що її формують, і забезпечення їхньої ефективної діяльності як суб’єктів міжнародного співробітництва.

Загрози інформаційного складника економічної безпеки галузі умовно можна класифікувати за чотирима основними групами.

Інформаційні – недостатність інформації; відсутність систем кваліфіковано збору, аналізу, оцінки, обробки використання та збереження інформації; недостатність, неповнота інформації, необхідної для прийняття рішень; наявність асиметричної інформації; порушення регламентів інформаційного обміну; проникнення в інформаційні системи та незаконне збирання і використання інформації; дезінформація споживачів внутрішнього ринку, суспільства, споживачів, міжнародної спільноти; несанкціонований доступ до інформаційних ресурсів, незаконне вилучення інформації; приховування інформації, несанкціонованого розкриття та використання інформації;

ознаки інформаційної війни проти країни та її економічної системи як інформаційного супроводу політичних та військових конфліктів.

Фізичні – порушення роботи чи знищення засобів оброблення та носіїв інформаційних ресурсів, їх розкрадання, пошкодження чи розкриття апаратних або програмних ключів доступу; недостатність кваліфікації персоналу, що опрацьовує інформацію; пошкодження інформаційних мереж, програмного забезпечення.

Технічні – перехоплення інформації в лініях зв’язку та її зміна та інші зовнішні технічні втручання в роботу інформаційних систем всіх рівнів.

Програмні – розповсюдження вірусних програм, знищення модифікації відомостей, що використовуються в інформаційних системах.

Інформаційна безпека та необхідність її забезпечення стають нагальними потребами на всіх рівнях розвитку суспільних систем, оскільки широкомасштабний розвиток інформаційних систем та комп’ютеризація привели до завантаження всієї основної інформації про матеріальні та нематеріальні ресурси, фінансові, кадрові ресурси, фінансово-господарську діяльність на всіх рівнях та навіть державне управління і законодавство у всіх аспектах створення, збереження, обміну, використання інформації із площини документальної, паперової у площину електронної інформації та документообігу, що збільшило можливості несанкціонованого доступу до неї з метою незаконного ознайомлення, використання, оприлюднення чи зміни.

Якщо раніше обіг інформації був значно безпечнішим, то сьогодні це – один із найбільш вразливих елементів у забезпеченні безпеки будь-якої системи. На рівні окремих підприємств, компаній, холдингів, фінансово-промислових груп чи інших господарчих структур, що входять та формують галузі в нашій країні, цю проблематику розуміють та вирішують її в межах своїх завдань та ресурсів, вважаючи це частиною комплексу забезпечення економічної безпеки. На жаль, на рівні країни за Методиками розрахунку рівня економічної безпеки країни як 2003-го, так і 2007-го та 2013 року інформаційну безпеку навіть не визначено як складник економічної безпеки країни, що говорить про недостатнє усвідомлення глибини та масштабів загроз. У цьому контексті виникає багато питань, які будуть лише активізуватися у майбутньому.

Інформаційна безпека галузі має вирішувати такі завдання, як:

– виявлення загроз інформаційним ресурсам та інформаційним системам підприємств галузі, оцінювання цих загроз та опрацювання комплексу дій із їх нейтралізації;

– організація та функціонування механізму захисту державної, комерційної, службової та особистої інформації і комерційної таємниці;

– захист прав юридичних осіб галузі на інтелектуальну власність та протидія її незаконному отриманню і використанню;

– організація процесу безпечного збору, обробки, використання та збереження інформації, що використовується як окремими підприємствами галузі, так і галузевими об'єднаннями.

Загрози інформаційному складнику економічної безпеки галузі можна класифікувати за такими критеріями:

– за елементами інформаційних систем (загрози та небезпеки, спрямовані на програми, сервери, інформаційні бази даних, апаратуру, мережі тощо);

– за концептуальними аспектами інформаційної безпеки (такими як доступність, комплексність, цілісність, оперативність тощо);

– за джерелом загроз (внутрішні та зовнішні загрози);

– за засобом здійснення (випадкові, навмисні, техногенні та ін.).

Основу інформаційного складника економічної безпеки галузі формують складові фактори стану та рівня інформаційної безпеки окремих підприємств, що входять до складу галузі як підсистеми загальної системи. Найбільш розповсюдженими загрозами інформаційній безпеці підприємств є загрози, пов'язані із помилками, викликаними роботою користувачів, помилками в обслуговуванні інформаційних систем; крадіжки та підробки інформаційних даних; відмови в інформаційних системах; недостатність для обробки даних та інформаційного обміну наявної інформаційної інфраструктури; недостатній рівень підготовки кадрів для роботи із інформаційними ресурсами; низька технологічність наявного обладнання; відсутність чи недостатність необхідної технічної підтримки; порушення правил експлуатації, вихід із ладу апаратури через фізичне чи моральне зношення; надмірний обсяг інформації, що опрацьовується; використання неліцензійного програмного забезпечення; неузгодження наявного програмного забезпечення та даних наявних інформаційних ресурсів; від-

мова апаратного та програмного забезпечення; застосування спеціальних та технічних методів, як знищують інформацію чи видозмінюють її; збої в роботі обслуговуючої інфраструктури мереж, забезпечення кліматичного режиму, кондиціонування; знищення інформаційних даних, розповсюдження та дія програмних вірусів; внесення змін в інформацію під час її обробки; вилучення інформації, диверсії.

Висновки. Основними зовнішніми загрозами економічній безпеці галузі насамперед є загрози, пов'язані з відсутністю інформації як такої про діяльність підприємств галузі, продукцію галузі та адекватного представлення інформації про неї на зовнішніх ринках у світовому інформаційному просторі. Також небезпеку являє собою деструктивна інформація про діяльність галузі країни та її продукцію або дезінформація, що являє собою умисно змінену, перекручену чи відверто неправдиву інформацію про діяльність галузі країни та підприємств, що її представляють, у світовому інформаційному просторі. Значну загрозу являють собою недостатня інтегрованість вітчизняних інформаційних ресурсів у світові інформаційні мережі та незначний вплив вітчизняного контенту у світовому інформаційному ринку; відсутність державної інформаційної політики як такої, що сприяла би втіленню стратегії європейської інтеграції країни, спрямованої на підтримку її власних галузей на світовому ринку; недостатній технічний та технологічний рівень інформаційної інфраструктури, що забезпечує її всіма видами інформаційних ресурсів та дає змогу створювати, акумулювати та обмінюватися інформацією в межах економічного, соціального, політичного та культурного процесів; низький рівень відповідальності за порушення норм безпеки інформації та інформаційних систем; недостатній захист інтелектуальної власності, в тому числі пов'язаний із створенням та використанням інформаційних ресурсів, та інші фактори.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Економічна безпека: навчальний посібник / [О.Є. Користін, О.І. Барановський, Л.В. Герасименко та ін.]; за ред. О.М. Джузі. – Алерта; КНТ; Центр учбової літератури, 2010. – 368 с.
2. Сухоруков А.І. Фінансова безпека держави / А.І. Сухоруков, О.Д. Ладюк. – К.: Центр учбової літератури, 2007. – 189 с.
3. Єрмошенко М.М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення / М.М. Єрмошенко. – К.: Київ. Нац. торг.-екон. ун-т., 2001. – 309 с.
4. Камлик М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект: Навч. посібник. – К.: Атака, 2005. – 432 с.
5. Костров А.В. Основы информационного менеджмента / А.В. Костров. – 2-е изд., перераб. и доп. – М.: Финансы и статистика, 2009. – 528 с.
6. Кригер В. Информационный менеджмент / В. Кригер. – Владивосток: [б. и.], 2004. – 176 с.
7. Гринберг А.С. Информационный менеджмент / А.С. Гринберг, И.А. Король. – М.: ЮНИТИ-ДАНА, 2003. – 415 с.
8. Лук'яненко Д.І. Розвиток інформаційного менеджменту як наукової категорії / Д.І. Лук'яненко // Науковий вісник Полтавського університету економіки та торгівлі. – 2013. – № 1(56). – С. 183–187.
9. Калініна Л.М. Генезис інформаційного менеджменту як галузі наукового знання / Л.М. Калініна // Стратегічні пріоритети. – 2009. – № 4(13). – С. 71–76.
10. Бобик О.І. Теорія ймовірностей і математична статистика / О.І. Бобик, Г.І. Берегова, Б.І. Копитко. – Львів: ЛБІ НБУ, 2003. – 101 с.