означає, що Національному банку України необхідно розробити довгостроковий план розвитку валютно-кредитних відносин в Україні, тобто впроваджувати дієву валютно-кредитну політику, розробка якої потребує існування загальнодержавного стратегічного довгострокового плану розвитку соціально-економічного стану України.

Список використаних джерел:

1. Барановський О. Антикризові заходи урядів і центральних банків зарубіжних країн / О. Барановський // Вісник НБУ. – 2009, квітень. – С. 8-19.
2. Даниленко А.І., Кошик О.М., Шульга О.Б., Василик О.Д., Савлук М.І. Фінансово-кредитні важелі регулювання економіки України в перехідний період / За ред. А.І. Даниленка. – К., 2009. – 242 с.
3. Лагутін В.Д. Вибір стратегії монетарної політики / В.Д. Лагутін, Т.О. Кричевська // Фінанси України. – 2009. – № 3. – С. 3-15.
4. Продан Т.Я. Грошово-кредитна політика у регулюванні грошового обігу в кризових умовах.// Збірник тез доповідей науково-практичної конференції 15-16 жовтня 2009 р. – Чернівці: ДрукАрт – 2009. – С.138-139.
5. Стецко Л.И. Денежно-кредитная политика как средство преодоления финансово-экономического кризиса // Меморандум про економічну і фінансову політику. – К. : Вид-во НБУ, 2008. – 236 с.

УДК 658.012

ІВАНЧЕНКО Н.О.,
Інститут економіки та менеджменту НАУ,
доцент кафедри економічної кібернетики, к.е.н.

ІНФОРМАЦІЙНА СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ТА ЇЇ ЗНАЧЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОГО РОЗВИТКУ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

Анотація. *У статті розглянуті сучасні загрози інформаційній безпеці підприємства. На основі аналізу практичного досвіду організації захисту інтересів господарюючих суб'єктів в інформаційній сфері запропонований концептуальний підхід до визначення функцій, завдань і організаційних основ функціонування підрозділів інформаційної безпеки підприємств з позицій загальних завдань безпеки бізнесу і забезпечення стійкого розвитку національної економіки.*

Ключові слова: економічна безпека, стійкий розвиток, інформаційна безпека, національна економіка, інформаційні технології.

Аннотация. *В статье рассмотренные современные угрозы информационной безопасности предприятия. На основе анализа практического опыта организации защиты интересов хозяйствующих субъектов в информационной сфере предложенный концептуальный подход к определению функций, заданий и организационных основ функционирования подразделений информационной безопасности предприятий с позиций общих заданийбезопасности бизнеса и обеспечения устойчивого развития национальной экономики.*

Ключевые слова: экономическая безопасность, устойчивое развитие, информационная безопасность, национальная экономика, информационные технологии.

Annotation. *In the article the considered modern threats to informative safety of enterprise. On the basis of analysis of practical experience of organization of defence of interests of being subjects in charge in an informative sphere offered conceptual approach to determination of functions, tasks and organizational bases of functioning of subsections of informative safety of enterprises from positions of commons tasks of safety of business and providing of steady development of national economy.*

Keywords: economic safety, steady development, informative safety, national economy, informations technologies.

Постановка проблеми. Одним із актуальних питань сучасності є проблема економічної безпеки як особистості, так і держави. Ситуація, що склалася тепер у світі і в нашій країні, породила безліч небезпек та загроз економічним відносинам, що формуються в Україні. Поняття економічної безпеки підприємства можна розглядати з кількох позицій. З позиції різних агентів ринку, що взаємодіють з підприємством (споживачів, суміжників, податкових, кредитних і т. ін.) [8]. В цьому разі можна визначити, що економічна безпека є комплексним відображенням ступеня надійності підприємства як партнера у виробничих, фінансових, комерційних та інших економічних відносинах за певний проміжок часу.

З позицій самого підприємства оцінка економічної безпеки полягає у визначенні рівня захищеності його потенціалу (виробничо-технічного, фінансового, соціального) і тенденцій його змін. При цьому під економічною безпекою слід розуміти захищеність його потенціалу від негативної дії зовнішніх і внутрішніх чинників, прямих або непрямих економічних загроз, а також здатність до відтворення.

Рівень економічної безпеки підприємства залежить від того, наскільки ефективно його керівництво та фахівці зможуть уникнути можливих загроз і ліквідувати шкідливі наслідки негативних складових зовнішнього та внутрішнього середовищ.

Отже, економічна безпека – це стан стійкого розвитку і здатність економічної системи протистояти небезпеці руйнування її організаційної структури і статусу, а також перешкодам у досягненні цілей розвитку.

Проблема пошуку шляхів стійкого розвитку останнім часом набуває все більш актуального характеру як в глобальному загальносвітовому аспекті, так і на національному, і регіональному рівнях.

Необхідною умовою переходу до моделі стійкого розвитку є збалансоване рішення задач вітчизняного виробничого комплексу. У числі останніх важливе місце займає проблема забезпечення стійкого розвитку українських підприємств.

Аналіз останніх досліджень і публікацій. Під "стійкістю" в економічній літературі розуміється "здатність системи виконувати роботу проти дії зовнішніх сил по збереженню, відтворенню і розвитку самої себе при зміні зовнішніх умов" [1]. "Стійкість підприємства" в економічному словнику А.Б. Борісова трактується як "фінансовий стан підприємства, господарська діяльність якого забезпечує в нормальних умовах виконання всіх його зобов'язань перед працівниками, іншими організаціями, державою, завдяки достатнім доходам і відповідним витратам" [2].

Метою статті є аналіз практичного досвіду організації захисту інтересів господарюючих суб'єктів в інформаційній сфері.

Виклад основного матеріалу. В умовах перехідної економіки далеко не всі підприємства можуть вийти на траєкторію стійкого розвитку і у такому разі в повній відповідності із законами ринку їм, рано чи пізно, доведеться зникнути під натиском конкурентів. Разом з тим, тільки забезпечивши накопичення певної критичної маси вітчизняних підприємств (включаючи всі системоутворюючі), що реалізували перехід до моделі стійкого розвитку, можна вести мову про можливість реалізації такої моделі стосовно національної економіки в цілому.

Проте, на шляху досягнення поставленої мети існує велика кількість перешкод і обмежень. Виходячи з цілей даної статті виділимо лише одну з таких обставин. Вона полягає в тому, що в реаліях сучасної української дійсності господарюючі суб'єкти вимушені вибудовувати стратегію свого виживання і розвитку в ринковому середовищі, що характеризується, з одного боку, широким розповсюдженням нецивілізованих форм конкуренції і значною криміналізацією економічних відносин, а з іншої - украй низькою ефективністю прав власності і контрактних зобов'язань. Все вищеперелічене обумовлює зростаючу увагу з боку бізнесу до проблем забезпечення власної економічної безпеки, які висуваються на пріоритетні позиції не тільки в кризові періоди, але і при роботі в режимі стійкого функціонування економіки [3].

При цьому все більш очевидною стає залежність загального рівня економічної безпеки підприємства від її інформаційної складової. Практика показує, що будь-яка цілеспрямована недружня акція, направлена проти інтересів господарюючого суб'єкта, починається із збору інформації. Основними причинами недосконалості вітчизняних систем інформаційної безпеки пояснюються тим, що [5]:

- інформація як матеріальна цінність порівняно з будь-якою іншою матеріальною цінністю відносно просто копіюється, модернізується або знищується;
- широкомасштабний розвиток та впровадження обчислювальної техніки та телекомунікаційних систем у рамках територіально розподіленої мережі, перехід на цій основі до безпаперової технології, збільшення обсягів і структурованості оброблювальної інформації, розширення кола її користувачів приводить до ускладнення можливості контролю та запобігання несанкціонованого одержання та використання інформації.

Саме тому, питання інформаційної безпеки вже давно входять до числа головних пріоритетів практично всіх крупних українських і світових компаній, а останніми роками все більше число керівників середнього і дрібного вітчизняного бізнесу починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією, системами її обробки і співробітниками, що беруть участь в цьому процесі.

Погіршення таких параметрів інформації (інформаційних ресурсів), як конфіденційність, цілісність, доступність, достовірність та ін., може привести до вельми негативних наслідків: збоям у функціонуванні систем управління технологічними процесами і інших критичних систем; до розголошування відомостей, що становлять комерційну таємницю і інші види таємниць; до порушення достовірності фінансової документації; до несанкціонованого доступу до персональних даних фізичних осіб і т. ін. Результатом перерахованого можуть стати: розрив (або погіршення) ділових відносин з партнерами; зрив переговорів, втрата вигідних контрактів; невиконання договірних зобов'язань; необхідність проведення додаткових ринкових досліджень; відмова від рішень, що стали неефективними із-за розголосу інформації, і, як наслідок, фінансові втрати, пов'язані з новими розробками; втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію; зниження цін або об'ємів реалізації; втрата авторитету або ділової репутації фірми; жорсткіші умови отримання кредитів; труднощі в постачанні і придбанні устаткування і т. ін. У певних ситуаціях зневажання питаннями захисту інформації може, як вже наголошувалося, привести і до повної втрати бізнесу.

Надійно захистити бізнес від перерахованих негативних явищ можна тільки на основі формування ефективної системи забезпечення інформаційної безпеки підприємства.

Особливо слід зазначити, що господарюючий суб'єкт - володар інформації – має право застосовувати заходи по захисту інформації, що становлять комерційну таємницю, під якою відповідно до чинного законодавства розуміється науково-технічна, технологічна, виробнича, фінансово-економічна або інша

інформація (зокрема секрети виробництва (ноу-хау)), яка має дійсну або потенційну комерційну цінність через невідомість її третім особам, до якого немає вільного доступу на законній підставі і відносно якої володарем такої інформації введений режим комерційної таємниці.

Таким чином, сучасна корпоративна система інформаційної безпеки покликана забезпечувати захист конфіденційної інформації від несанкціонованого доступу, запобігати зловмисним або випадковим змінам (контролювати цілісність) і надавати необхідний рівень доступності. Йдеться саме про систему, а не про окремі, нехай навіть дуже ефективні в своїй області, рішеннях.

Одним з найважливіших видів діяльності по забезпеченню інформаційної безпеки підприємства є виявлення, оцінка і запобігання загрозам інформаційним системам і інформаційним ресурсам. Вказані загрози можна умовно розділити на чотири основні групи:

програмні - впровадження "вірусів", апаратних і програмних закладок; знищення і модифікація даних в інформаційних системах;

технічні, в т.ч. радіоелектронні, - перехоплення інформації в лініях зв'язку; радіоелектронне придушення сигналу в лініях зв'язку і системах управління;

фізичні - знищення засобів обробки і носіїв інформації;

режимні - порушення регламентів інформаційного обміну; незаконні збір і використання інформації; несанкціонований доступ до інформаційних ресурсів; незаконне копіювання даних в інформаційних системах; розкрадання носіїв, а також апаратних або програмних парольних ключів; дезінформація, приховування або спотворення інформації; розкрадання інформації з баз даних.

Питання аналізу загроз і ризиків є таким, що визначається при побудові ефективної системи захисту інформації. Проте, за оцінками фахівців, лише не більше 7 % компаній використовують власні ("поглиблені") методики аналізу ризиків, які дозволяють виконувати кількісний аналіз і оптимізацію підсистеми інформаційної безпеки.

Тим часом, статистика у області інформаційної безпеки свідчить, що близько 80 % зловмисників належить до інсайдерів. У компаніях телекомунікаційної галузі на їх дії припадає близько 90 % фінансових втрат [7].

Навряд чи справедливо винити бізнес-керівництво в тому, що воно не усвідомлює самої проблеми інформаційної безпеки. Але багато директорів компаній можуть елементарно не "бачити" очевидного зв'язку між втратою доходів і незакритою "діркою" в системі інформаційного захисту. Тому в першу чергу необхідно представити проблему в зрозумілому для бізнесу вигляді. Це завдання лягає на керівництво служби економічної безпеки господарюючого суб'єкта, яке повинне виявити і наочно показати власникам (топменеджменту) підприємства весь спектр загроз в інформаційній сфері, а також переконати, що протистояти цим загрозам можна тільки на основі створення і впровадження ефективних систем захисту інформації.

Створюючи такі системи необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілого ряду різнорідних заходів, які можна розділити на три групи: юридичні, організаційно-економічні і технологічні. По-друге, хоча розробкою заходів захисту стосовно кожної з трьох груп безумовно повинні займатися фахівці відповідних областей знань, кожний з яких застосовує свої способи і методи для досягнення заданої мети, кінцевий успіх у визначальному ступені залежатиме від того, наскільки в рамках системного підходу вдається визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту.

Аналіз представлених в літературі різних поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки підприємства, дозволив сформулювати основні функції, завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки.

У сучасному представленні ролевих функцій служби інформаційної безпеки можна виділити чотири напрями [2]:

1) розробка методології і методик аналізу загроз, оцінки рівня інформаційної безпеки підприємства і корпоративних стандартів системи її забезпечення;

2) організація і здійснення конкретних видів діяльності по захисту інформації;

3) експлуатація технічних засобів захисту інформації;

4) аудит і контроль функціонування системи інформаційної безпеки підприємства.

В рамках першого напряму повинні розв'язуватися наступні основні завдання [2]:

1) аналіз і узагальнення потенційних загроз, причин порушень вимог інформаційної безпеки, що реалізувалися. Аналіз ступеня забезпечення безперервності процесів бізнесу, що використовують ІТ, з погляду питань інформаційної безпеки. Пошук нових загроз пов'язаних з інформаційною взаємодією;

2) побудова методик оцінки інформаційних ризиків;

3) інформаційне обстеження компанії і інформаційних ресурсів;

4) розробка методів захисту інформації та ІТ, а також методик їх впровадження в діяльність компанії;

5) розробка і модифікація концепції і політик забезпечення інформаційної безпеки. Створення локальної нормативної бази з цих питань з урахуванням комплексного підходу до економічної безпеки компанії;

6) розробка методик оцінки рівня інформаційної безпеки і визначення достатності захисту інформації і ІТ з урахуванням потреб бізнесу, а також існуючої і перспективної нормативної бази України;

7) розробка корпоративного стандарту забезпечення інформаційної безпеки компанії;

8) аналіз з погляду виконання вимог інформаційної безпеки всіх використовуваних в компанії процедур створення, обробки, пересилки, зберігання, знищення інформації, зокрема: процедур інформаційної взаємодії підрозділів компанії між собою і із зовнішніми організаціями; порядок доступу співробітників компанії і суміжних організацій, а також клієнтів до інформаційних ресурсів компанії і зовнішніх комп'ютерних мереж; проектів розвитку IT компанії, включаючи системи зв'язку і телекомунікацій; проектів договорів із зовнішніми організаціями, з якими здійснюється обмін інформацією; проектів інших нормативних документів компанії, які передбачають інформаційну взаємодію;

9) віднесення інформації до категорії обмеженого доступу (службова таємниця;

10) підготовка аналітичних записок, що містять висновки з проведеного аналізу і пропозиції по реалізації захисту інформації.

В рамках другого напряму повинні розв'язуватися наступні основні завдання:

1) планування на основі координації діяльності всіх підрозділів компанії робіт по забезпеченню інформаційної безпеки підприємства;

2) організація і участь у впровадженні методів забезпечення інформаційної безпеки в діяльність підприємства. Робота з персоналом компанії, партнерами і клієнтами (інструктаж, навчання і консалтинг; створення в колективі "атмосфери інформаційної безпеки ");

3) узгодження: заявок на доступ і порядок доступу співробітників компанії і зовнішніх організацій до інформаційних ресурсів компанії; узгодження «матриці доступу», ролей в IT; процедур інформаційної взаємодії підрозділів компанії між собою і із зовнішніми організаціями; проектів розвитку IT-інфраструктури компанії, включаючи системи зв'язку і телекомунікацій; договорів із зовнішніми організаціями, з якими здійснюється інформаційна взаємодія; проектів наказів, розпоряджень, порядків взаємодій, інших нормативно-розпорядчих документів компанії, в яких зачіпаються питання IT і інформаційної взаємодії;

4) участь в тестуванні, випробуваннях і прийманні інформаційних систем, систем зв'язку і телекомунікацій. Підготовка висновків;

5) розвиток комплексної системи інформаційної безпеки у філіалах, дочірніх структурах;

6) рішення поточних практичних питань по інформаційній безпеці, що виникають в підрозділах компанії, її філіалах і дочірніх структурах.

В рамках третього напряму повинні розв'язуватися наступні основні завдання:

1) підтримка ключових структур, використовуваних в зовнішніх і вбудованих засобах криптографічного захисту інформації;

2) забезпечення роботи інфраструктури відкритих ключів компанії;

3) забезпечення працівників компанії індивідуальними засобами аутентифікації, підтримка їх працездатності;

4) рішення вказаних вище задач у філіалах, дочірніх компаніях;

5) підтримка роботи інших засобів інформаційної безпеки (міжмережевих екранів, IDS (IPS), різних «агентів» безпеки і т.д.).

В рамках четвертого напряму повинні розв'язуватися наступні основні завдання:

1) перевірка виконання вимог інформаційної безпеки працівниками компанії і іншими особами, що мають доступ до інформаційних ресурсів компанії;

2) моніторинг дій користувачів IT компанії (несанкціонованої модифікації критичної інформації, використання різних поштових і інших сервісів мережі Інтернет для відправки конфіденційної інформації за межі компанії і т. д.).

3) контроль своєчасної зміни прав користувачів в інформаційних системах компанії; блокування облікових записів звільнених (переведених на іншу роботу) користувачів; зміни групових засобів аутентифікації користувачів після звільнення члена групи. Контроль дотримання безпеки, включаючи парольну політику, інші вбудовані системи інформаційної безпеки, зовнішні засоби захисту інформації;

4) моніторинг роботи систем виявлення (запобігання) мережевих атак, систем оцінки якості (з погляду інформаційної безпеки) побудови мережі і інших автоматизованих систем комп'ютерної безпеки;

5) участь в ліквідації виявлених порушень інформаційної безпеки і вимог нормативних документів з цих питань. Підготовка пропозицій по попередженню порушень;

6) проведення внутрішнього аудиту питань інформаційної безпеки. Підготовка пропозицій по використанню зовнішнього аудиту;

7) проведення робіт з підготовки компанії до сертифікації за міжнародними стандартами безпеки IT;

8) проведення моніторингу можливого просочування конфіденційної інформації по технічних каналах.

Враховуючи міждисциплінарний характер питань, що входять в блок інформаційної безпеки, деякі з перерахованих функцій можуть виконуватися тільки спільно з іншими структурними підрозділами підприємства (підрозділами IT, службою по роботі з персоналом, юридичною, господарською службою і т.д.).

З різних організаційних схем функціонування підрозділів, що відповідають за інформаційну безпеку підприємства (функції такого підрозділу покладаються на системних і прикладних адміністраторів; вказаний підрозділ знаходиться в структурі IT служби, служби економічної безпеки підприємства, чи ж є самостійною структурною одиницею компанії, що підкоряється вищому керівництву), найбільш дієвим представляється варіант, при якому підрозділ інформаційної безпеки входить до складу служби економічної безпеки

підприємства. Саме в цьому випадку створюються якнайкращі можливості рішення проблем інформаційної безпеки в контексті загальних завдань безпеки бізнесу.

Інформаційна безпека тісно пов'язана з функціями інформаційного ринку, найбільш розгалуженою частиною якого є "сфера інформації", а головним сектором виступає економічна інформація, що, у свою чергу, безпосередньо пов'язана з проблемою забезпечення економічної безпеки країни загалом, різних суб'єктів господарювання, особистості.

Світовий досвід розвитку інформаційного ринку свідчить, що управлінська і підприємницька діяльність потребує постійного отримання економічної інформації, а також інформації соціального характеру.

Зважаючи на зазначене під інформаційною безпекою слід розуміти такий стан інформаційного середовища (інформації, інформаційної системи, інформаційного ресурсу), за якого гарантується розвиток цього середовища та його використання в інтересах людини, суспільства та держави, а також захищеність від відповідних загроз.

Висновок. Відзначимо, що в сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. У свою чергу, надійне забезпечення економічної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але і національної економіки в цілому.

Список використаних джерел:

1. Мартынов А.С., Артюхов В.В., Виноградов В.Г. Устойчивое развитие и приоритеты природоохранного инвестирования в регионах России. М.: Practical Scince, 2000. С. 2.

2. Борисов А.Б. Большой экономический словарь. М.: Книжный мир, 2001. С. 631.

3. Економічна безпека : навч. посіб. / за ред. З.С. Варналія. – К. Знання, 2009. – 647 с.

4. М.М. Зацеркляний, О.Ф. Мельников Основи економічної безпеки : Навчальний посібник. – К. : КНТ, 2009. – 337с.

5. Економічна безпека : навч. посіб. / О. Є. Користін, О.І. Барановський, Л. В. Герасименко та ін.; за ред. О. М. Джужі. – К. Алерта; КНТ; Центр учбової літератури, 2010. – 368 с.

6. Олейников Е.А. Экономическая и национальная безопасность: [Текст]: учебник для вузов / Е. А. Олейников. – Экзамен, 2005. – 768 с.

7. Сафрончук М.В. Экономическая безопасность и инвестиции как фактор роста переходной экономики России / М.В. Сафрончук // Вопросы статистики. – 2001. – №11. – С. 50-55.

8. Економічна безпека підприємств, організацій установ : Навч. посібник [для студ. вищ. навч. закл.]. / [В. Л. Ортинський, І.С. Керницький, З. Б. Живко та ін.]; – К. : Правова єдність, 2009. – 544 с.

УДК 338.2 (477)(045)

ДУДЧАК А.В.,
Киевский национальный торгово-экономический университет,
кафедра международной экономики, к.э.н.

ЭКОНОМИЧЕСКАЯ СТРАТЕГИЯ УКРАИНЫ: МИФЫ И РЕАЛЬНОСТЬ

Аннотация. *В статье рассматриваются реальные последствия внешнеэкономической политики и стратегии Украины в контексте развития интеграционных процессов на постсоветском пространстве. А также возможные последствия интеграционного сотрудничества Украины с Европейским Союзом или в рамках Таможенного союза.*

Ключевые слова: Таможенный союз, Зона свободной торговли, Европейский Союз, интеграция, импорт, экспорт.

Annotation. *In the clause real consequences of the external economic policy and strategy of Ukraine in a context of development of integration processes on the post-Soviet territory are considered. And also possible consequences of integration cooperation of Ukraine with European Union or within the limits of Customs union.*

Keywords: Customs union, Free trade area, European Union, integration, import, export.

Сегодня Украина стоит перед выбором, важность которого сложно сопоставить с каким-либо событием за весь период после развала Советского Союза. Выбор направления вектора интеграции – Зона свободной торговли с Евросоюзом или Таможенный союз с Россией, Беларусью и Казахстаном – это решение, которое определит перспективы развития страны на десятилетия. И ответ на вопрос: будет ли вообще, это развитие? От этого решения, на принятие которого остаются считанные месяцы, зависит – сможет ли Украина сохранить остатки своего научно-технического потенциала и в перспективе стать развитой державой, или ее судьба превратиться в ресурсный придаток Западной Европы с деградирующим населением.

Даже бараны чувствуют предстоящую гибель, когда их ведут на бойню, и оглашают окрестности предсмертным ревом. Те, кто это наблюдал, говорят – жуткое зрелище. Население Украины, подвергаемое на