УДК 658.586

ВАСИЛЬЦІВ Т. Г., МАКСИМЮК С. О.
Львівський торговельно-економічний університет
КЕРНИЦЬКИЙ І. С.
SGGW, Варшава, Польща

СУТНІСНІ ХАРАКТЕРИСТИКИ ТА НАПРЯМИ ФОРМУВАННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

У статті розглянуто особливості формування системи економічної безпеки суб'єктів господарювання, досліджено та здійснено класифікацію елементів системи економічної безпеки підприємств, оцінено вплив загроз на інформаційну безпеку суб'єктів господарювання та надано рекомендації щодо запобігання загрозам підприємств в економічній сфері.

Ключові слова: економічна безпека, суб'єкт господарювання, елементи економічної безпеки, інформаційна безпека.

VASYLTSIV T. G., MAKSUMIYK S. O.
University of Trade and Economics
KERNYTSKYY I. S.
Warsaw University of Life Sciences WULS (SGGW)

THE MAIN CHARACTERISTICS AND WAYS OF FORMATION OF THE ECONOMIC SECURITY SYSTEM OF THE ENTITIES

In this article the concept of economic security entities, its goals and functional goals. Formulated value system of economic safety entities and the peculiarities of its formation, purpose and principles of creation. The authors found that the system of economic security each entity is an individual, its fullness and effectiveness depend on the state of the current legal framework, the volume of logistical and financial resources allocated for these purposes, from understanding the importance of each employee security business and - the experience and efficiency of service managers to ensure economic security. Investigated and the classification system elements of economic security entities. The ways of development of information security of data subjects. Also highlighted legal, software and technical and organizational security threat to economic entities assessed their impact on information security, and developed a series of recommendations to prevent such threats every business in the economic sphere.

Keywords: economic security entity, the elements of economic security, informational safety.

Постановка проблеми

Актуальність дослідження визначається високою актуальністю та своєчасністю постановки проблеми адаптації вітчизняних суб'єктів господарювання до умов ринкового середовища, нестабільністю зовнішнього середовища і поглибленням внутрішніх загроз, що призводить до зниження рівня економічної безпеки (ЕБ) підприємств в Україні, від рівня якої залежать кінцеві результати їх господарювання, фінансовий стан та конкурентоспроможність.

Діяльність багатьох суб'єктів господарювання характеризується нестабільністю динаміки розвитку і потребує швидкої адаптації до сучасних умов господарювання. Кожен суб'єкт господарювання повинен підпорядковуватися законам розвитку і виживання, обліку невизначеності і нестійкості економічного середовища, кон'юнктури споживчого ринку тощо. Однак, навіть, адаптуючи ці фактори до реалій сучасного бізнесу, неможливо досягти ідеально безпечного середовища комерційної діяльності, тому доцільно розглядати економічну безпеку як стан, за якого мінімізується негативний вплив внутрішніх і зовнішніх загроз на діяльність та економічний результат підприємства. Все це зумовлює необхідність формування і управління системою економічної безпеки.

Аналіз останніх досліджень і публікацій

Істотний внесок у дослідження теоретичних та прикладних аспектів системи ЕБ суб'єктів господарювання внесли такі відомі вітчизняні науковці, як Браіловський М. М., Дорошко В. О., Чирков Д. В., Шелест М. Е., Ортинський В. Л., Живко З. Б., Копитко М. І. Проте, слід зауважити, що існує низка питань, що стосуються науково-методичного висвітлення сутності та характеристик напрямів формування системи економічної безпеки суб'єктів господарювання, які й досі залишаються невирішеними.

Виокремлення невирішених аспектів загальної проблеми

Аналіз наукової літератури із зазначеної проблематики свідчить про те, що окремі питання, пов'язані з визначенням системи економічної безпеки та захисту її структурних елементів, досліджено недостатньо. Саме тому, визначення нових наукових підходів щодо проблем реалізації системи ЕБ суб'єктів господарювання (СГ) потребує додаткового дослідження.

Формування цілей статті

Метою статті є висвітлення поняття, завдань та цілей системи економічної безпеки і розроблення рекомендацій щодо захисту її функціональних елементів.

Виклад основного матеріалу дослідження

Економічна безпека СГ – це стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації

і технологій, техніки та устаткування, прав) і підприємницьких можливостей, за якого гарантовано найефективніше їх використання для стабільного функціонування та динамічного науково-технічного й соціального розвитку, запобігання внутрішнім і зовнішнім негативним впливам.

Головною метою ЕБ СГ є гарантування їх стабільного і максимально ефективного функціонування та високий потенціал розвитку підприємств у майбутньому.

Для досягнення сформованої мети ЕБ СГ доцільно виокремити такі функціональні цілі як:

• забезпечення високої фінансової ефективності роботи і фінансової стійкості та незалежності підприємства;

• забезпечення технологічної незалежності та досягнення високої конкурентоспроможності технічного потенціалу;

• досягнення високої ефективності менеджменту оптимальної та ефективної організаційної структури управління підприємством;

• мінімізація руйнівного впливу результатів виробничо-господарської діяльності на стан навколишнього середовища;

• забезпечення високого рівня кваліфікації персоналу та його інтелектуального потенціалу належної ефективності корпоративних науково-дослідних та дослідно-конструкторських робіт (НДДКР);

• якісна правова захищеність усіх аспектів діяльності підприємства;

• забезпечення захисту інформаційного поля, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів підприємства.

Для досягнення поставленої мети та цілей на СГ створюється система економічної безпеки (СЕБ), яка являє собою сукупність внутрішніх і зовнішніх суб'єктів забезпечення ЕБ, всіх її власних ресурсів, зокрема організаційно-адміністративних, інтелектуальних, правових, матеріально-технічних і фінансових, які використовуються або можуть бути використані для комплексної протидії зовнішнім і внутрішнім небезпекам та загрозам для стабільної роботи і розвитку підприємства [1].

Система економічної безпеки кожного СГ є індивідуальною, її наповненість і дієвість залежать від чинної в державі законодавчої бази, від обсягу матеріально-технічних і фінансових ресурсів, призначених на ці цілі, від розуміння кожним з працівників важливості гарантування безпеки бізнесу, а також від досвіду та оперативності роботи керівників служб забезпечення ЕБ підприємств [2].

Головне завдання СЕБ СГ – передбачення і випередження можливих загроз, які призводять до кризового стану, а також, проведення антикризового управління, яке спрямоване на виведення підприємства з кризового стану; мінімізація зовнішніх і внутрішніх загроз економічному стану суб'єкта підприємництва, зокрема, його фінансовим, матеріальним, інформаційним, кадровим ресурсам на основі розробленого комплексу заходів економіко-правового і організаційного характеру [3].

В основу функціонування СЕБ закладено певні принципи, серед яких основними є:

1. Системність, згідно з якою під час організації ЕБ немає "важливих" та "неважливих" елементів. Небезпека, як рідина, проникає в економічну систему через кожну невелику щілину.

2. Обґрунтованість, обмеженість ресурсів захисту, як і всіх інших економічних ресурсів, вимагає глибокого науково-технічного обґрунтування рішень щодо забезпечення економічної безпеки.

3. Достатність. Вибирати потрібно такі засоби економічного захисту, які є достатніми, щоб протидіяти небезпеці. Водночас не потрібно витрачати зайві кошти. Щоразу, коли вирішується питання захисту від безпосередньої загрози, суб'єкт вибирає модель поведінки щодо небезпеки з огляду примус, протидію, стримування і узгодження. Вибір конкретної моделі визначається рівнем небезпеки.

4. Гнучкість – це здатність суб'єкта економічної діяльності швидко міняти модель забезпечення безпеки залежно від характеру та динаміки розвитку небезпеки.

5. Своєчасність. Суб'єкт ЕБ повинен мати відпрацьовані моделі захисту щодо рівня розвитку небезпеки і своєчасно застосовувати їх у поєднанні з моніторингом до конкретного стану небезпеки.

6. Бажання захищатися. Не завжди окремі суб'єкти економічної діяльності бажають захищати власні економічні об'єкти. Насамперед, це притаманне злочинним елементам у структурах менеджменту або проявляється в небажанні захищати загальну структуру її окремими складовими частинами. Це наслідок суперечностей між окремими структурами економічних систем, незбалансованості систем власності та влади між центральними і периферійними, інституційними та виконавчими елементами системи.

7. Уміння захищатися. Бажання захищатися має доповнюватися умінням.

Система забезпечення економічної безпеки суб'єктів господарювання залежно від структури власності, конкретних умов (масштабів фінансово-господарської діяльності, обсягів виробництва, територіальних особливостей, кадрового потенціалу тощо) повинна мати збалансований бюджет забезпечення, опираючись на який, вона буде зможе якісно виконувати свої завдання, а також нормативно-правове забезпечення, зокрема, діяльність служб організації, засоби, методи, нормативні документи, що визначають статус СЕБ та вимоги, які є обов'язковими в рамках сфери її дії [4]. Основні елементи СЕБ підприємства подано на рисунку 1.

Умовно всі елементи системи економічної безпеки можна розмежувати на ті, що передбачають фізичні способи запобігання загрозам, та ті, що базуються на інформаційних способах запобігання загрозам.

Рис. 1. Елементи системи економічної безпеки суб'єктів господарювання

Отже, для досягнення ефективності СЕБ доцільно визначити шляхи розроблення системи інформаційної безпеки (ІБ) СГ.

У постіндустріальному суспільстві, інформація, що стосується усіх напрямків діяльності підприємства, стає найціннішим і найдорожчим ресурсом, а проблеми інформаційної безпеки – складнішими і практично значущішими. ІБ є однією із складових частин економічної безпеки, яка формує дієву модель захищеності підприємства [5].

Створення ефективної системи ІБ є неможливим без чіткого визначення загроз інформації, що охороняється.

Основними загрозами ІБ є: її розголошення, витік і несанкціонований доступ до її джерел. З урахуванням викладеного вище, доцільно розглянути питання пов'язані з передумовами неправомірного оволодіння конфіденційною інформацією. Наші дослідження показали, що існують такі види загроз інформаційної безпеки [6]:

– розголошення (зайва балакучість співробітників) – 32 %;

– несанкціонований доступ шляхом підкупу і схиляння до співробітництва з боку конкурентів і злочинних угруповань – 24 %;

– відсутність на фірмі належного контролю і жорстких умов забезпечення інформаційної безпеки – 14 %;

– традиційний обмін виробничим досвідом – 12 %;

– безконтрольне використання інформаційних систем – 10 %;

– наявність передумов виникнення серед співробітників конфліктних ситуацій – 8 %.

Для попередження цих загроз, суб'єктам господарювання необхідно розробляти та впроваджувати у практику діяльності СГ методи: правові, програмно-технічні та організаційні [7].

Ми вважаємо, що актуальними правовими методами для діяльності СГ є обов'язковий запис в засновницьких та організаційних документах, у контрактах, що укладаються із співробітниками, в посадових інструкціях, положень та зобов'язань щодо захисту відомостей, що складають таємницю підприємства та його партнерів, формулювання і доведення до відома всіх співробітників підприємства механізму правової відповідальності за розголошення конфіденційних відомостей. До правового елементу системи захисту можна зараховувати страхування цінної інформації від різних ризиків. До них належать чинні в країні закони, укази, положення, інструкції та інші нормативні акти, які регламентують правила поводження з інформацією обмеженого використання і відповідальність за їх порушення та перешкоджають несанкціонованому використанню інформації і є стримуючим фактором для потенційних порушників.

Програмно-технічні методи, на нашу думку, необхідно реалізовувати за допомогою засобів програмного та апаратного забезпечення. Технічні методи захисту ІБ передбачають використання засобів програмно-технічного характеру, спрямованих, передусім, на обмеження доступу користувача, який працює з інформаційними системами підприємства, до тих інформаційних ресурсів, звертатися до яких він не має права. З таких засобів ми рекомендуємо використовувати:

• міжмережеві екрани (Firewall) — для блокування атак із зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall від компанії Nortel Networks). Вони управляють проходженням мереженого трафіка відповідно до правил (policies) безпеки. Як правило, міжмережеві екрани встановлюються на вході мережі й розділяють внутрішні (часткові) і зовнішні (загального доступу) мережі;

• системи виявлення вторгнень (IDS – Intrusion Detection System) — для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу "відмова в обслуговуванні" (Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі;

• засоби створення віртуальних приватних мереж (VPN – Virtual Private Network) — для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування.

Важливим також є захист периметра ІБ суб'єкта господарювання; для його охорони необхідно створити:

• системи охоронної й пожежної сигналізації;

• системи цифрового відеоспостереження;

• системи контролю й керування доступом.

Захист інформації від її витоку технічними каналами зв'язку на підприємстві можна забезпечити такими засобами та заходами:

• використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;

• установкою на лініях зв'язку високочастотних фільтрів;

• побудовою екранованих приміщень («капсул»);

• використанням екранованого устаткування;

• установкою активних систем зашумлення.

Вище було відзначено, що значна кількість конфіденційної інформації виходить за межі підприємства від самих працівників, тому суб'єкту господарювання доцільно впровадити такий організаційний захід як "Акт про нерозголошення інформації", який затверджує керівник підприємства. Ми пропонуємо внести до такого акту наступні пункти:

1. Співробітникам забороняється розголошувати загальні відомості комерційного характеру:

1.1. Загальні дані про СГ, її слабкі та сильні сторони.

1.2. Детальний опис структури, організації та ефективності служби безпеки на СГ.

1.3. Дані про постачальників і клієнтів.

1.4. Дані про ринки і способи збуту.

1.5. Умови, нюанси і методика фінансової діяльності.

1.6. Технологічні і промислові секрети.

1.7. Перелік заходів, здійснених СГ щодо своїх конкурентів.

1.8. Дані про справжніх і потенційних партнерів СГ, з метою перевірки їх на можливу співпрацю.

1.9. Інформація про час і маршрути перевезення вантажів та місце їх зберігання.

1.10. Виявлення уразливих ланок серед співробітників, тобто виявлення осіб, перспективних для вербування шляхом підкупу чи шантажу.

1.11.Зв'язки, можливості і ресурси керівництва компанії.

1.12. Виявлення кола постійних відвідувачів.

1.13. Інші відомості комерційного характеру.

2. Співробітникам забороняється розголошувати відомості особистого характеру:

2.1. Джерела і розмір доходів (свій і будь-кого із співробітників).

2.2. Уклад особистого життя керівництва організації і членів їх сімей.

2.3. Розклад і адреси ділових та особистих зустрічей керівництва.

2.4. Розмір фінансових ресурсів.

2.5. Інформацію про слабкості і людські пристрасті будь-кого із співробітників.

2.6. Згубні пристрасті і шкідливі звички співробітників.

2.7. Способи і маршрути пересування.

2.8. Інформація про місця зберігання грошей і цінностей.

2.9. Реальне місце проживання.

2.10. ІТ-безпеку.

3. Співробітникам, які мають доступ до інформаційної бази даних забороняється:

3.1. Пускати за свій комп'ютер осіб, непрацюючих у цій організації (зокрема і близьких родичів) і співробітників, право доступу, яких до інформаційних ресурсів обмежено.

3.2. Виносити інформацію з організації на будь-яких видах носіїв (зокрема передавати по електронній пошті), а також передавати особам, непрацюючим у цій організації, або доступ яких до цієї інформації обмежений.

3.3. Не допускати наявності вільних мережевих дротів у коридорах і місцях без відеоспостереження (тому що є можливість підключення ноутбука тощо).

3.4. Усім працівникам, які мають доступ до мережевих ресурсів, категорично забороняється розголошувати свій пароль (якщо він є).

3.5. Обмежити доступ всього персоналу до інформаційних ресурсів керівника та головного бухгалтера організації.

3.6. Як захист від комп'ютерних вірусів необхідно встановити на всіх комп'ютерах організації антивірусні програми з періодичним оновленням вірусної бази.

Забезпечення інформаційної безпеки повинно носити системний характер, тобто різні засоби захисту: правові, програмно-технічні та організаційні повинні використовувалися одночасно і під єдиним управлінням.

Висновки та перспективи подальших досліджень

Питання безпеки повинні завжди стояти на першому місці на будь-якому підприємстві. Економічна безпека – поняття багатогранне, вона охоплює багато функціональних складових, за умови дотримання яких забезпечується продуктивне функціонування підприємства.

Для забезпечення стабільного та ефективного функціонування СГ система економічної безпеки повинна бути розроблена відповідно до його специфіки, сфери діяльності та фінансових можливостей. ЕБ розробляють, враховуючи реальні та потенційно можливі небезпеки і загрози для діяльності СГ, а також з огляду на специфіку діяльності та особливості самого підприємства, тобто існуючих у нього можливостей і прагнень створити систему економічної безпеки високого рівня.

Нами було визначено, що складові СЕБ можна умовно поділити на фізичні та інформаційні, а оскільки інформаційна безпека підприємств набуває актуальності та щораз більшої важливості, нами було запропоновано систему забезпечення інформаційної безпеки, яка повинна використовувати правові, програмно-технічні та організаційні методи. Серед правових методів ми вважаємо за необхідне, створити механізм правової відповідальності за розголошення конфіденційних відомостей у всіх сферах ведення документації, а також рекомендуємо керівництву закладу застрахувати цінну, на їхню думку, інформацію.

Програмно-технічні методи повинні реалізовуватися за рахунок впровадження на підприємстві сучасної моделі користування комунікаційними системами мережевого захисту інформації, до складу яких входять мережеві екрани, системи виявлення вторгнень, засоби створення віртуальних приватних мереж.

Стосовно організаційних методів, пропонується впровадити “Акт про нерозголошення інформації”, з яким повинні бути ознайомлені “під особистий підпис” усі працівники підприємства.

Література

1. Економічна безпека підприємств, організацій та 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.

2. Степаненко А. В. Оцінка економічної безпеки України та її регіонів / А. В. Степаненко, М. І. Герасимов // Регіональна економіка. – 2002. – № 2. – С. 39–54.

3. Худолій Л. М. Складові економічної безпеки суб'єктів господарської діяльності / Л. М. Худолій // Ефективна економіка. – 2011. – № 1.

4. Економіка підприємства : підручник / за ред. С. Ф. Покропивного. – К. : КНЕУ, 1999.

5. Браіловський М. М. Захист економічної інформації : навч. посіб. / М. М. Браіловський, В. О. Дорошко, Д. В. Чирков, М. Е. Шелест ; за ред. проф. В. О. Хорошка. – К. : НАУ, 2002. – 78 с.

6. Колодюк А. В. Теоретичне обгрунтування поняття та виникнення інформаційного суспільства / А. В. Колодюк // Борисфен. – 2004. – № II. – С. 18–19.

7. Шаповал О. В. Розробка національних стратегій інформаційного розвитку – пріоритет сучасності О.В. Шаповал // Нова парадигма. – К., 2004. – Вип. 38. – С. 166–172.

Надійшла 15.05.2017; рецензент: д. е. н. Флейчук М. І.