УДК 351.746.1

ІНФОРМАЦІЙНА СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Міщенко С.П., к.е.н., доцент (ХНАДУ)

В статті розкрито принципи функціонування системи інформаційної безпеки підприємства та досліджено етапність створення системи захисту інформаційних ресурсів підприємства.

Ключові слова: економічна безпека, інформаційні ресурси, підприємство.

Актуальність теми дослідження. В реаліях сьогочасної української дійсності, що характеризуються високим рівнем нестабільності зовнішнього та внутрішнього середовища, підприємства змушені будувати стратегію власного виживання в ринковому середовищі, засновану на широкому застосуванні інформаційних технологій, одним із основних багатств економічно розвинутих держав. Адже, інформатизація економіки, проникнення її у всі сфери діяльності людини та держави, призвели до того, що економічний потенціал будь-якого суб'єкта все в більшій мірі став визначатися рівнем розвитку інформаційних структур, впливу якого пропорційно зростає й потенційна уразливість економіки.

Інформаційні технології розширили коло можливостей підприємств, забезпечили прискорення процесів обміну та співпраці, відкрили доступ до більш ефективних методів управління, однак,одночасно, й створили умови для підриву власної економічної безпеки підприємств, зниження рівня стабільності їх фінансово-економічної діяльності. Інформація із фактора забезпечення ефективності виробництва перетворилася на один із засобів конкурентної боротьби, володіючи яким, підприємство здатне не тільки отримати реальний прибуток від її використання, але й забезпечити стабільність свого розвитку. Це ще раз підтверджує справедливість висловлювання: «Хто володіє інформацією, той володіє світом». За таких умов набувають актуальності питання захисту інформаційної складової економічної безпеки підприємства.

Аналіз останніх досліджень та публікацій. Питанням забезпечення економічної безпеки приділяють значну увагу вітчизняні та зарубіжні науковці Л.І.Донець, В.І. Мунтіян, Г.В. Козаченко, В.П. Пономарьов, О.М. Ляшенко , Г. Пастернак-Таранушенко, В.Т. Шлемко і Ф.І. Бінько [1-5] та ін.., якими розроблено як понятійно-категоріальний апарат економічної безпеки, так і розроблено механізм її реалізації. Однак, не дивлячись на це в умовах випереджаючого розвитку інформаційних технологій потребує уваги питання вивчення інформаційної складової економічної безпеки підприємства, як фактора забезпечення економічної стабільності підприємства. Саме тому, ***метою даної статті*** є дослідження особливостей формування ефективної системи забезпечення інформаційної складової економічної безпеки підприємства.

Виклад основного матеріалу дослідження. Сучасний конкурентний механізм ринкового середовища побудований таким чином, що для забезпечення високих конкурентних позицій, власної економічної стабільності, підприємства змушені вдаватися до недобросовісних форм та методів боротьби, заснованих на відкритих протиборствах, знищенні матеріальних цінностей, привласненні та захопленні чужої власності. Це викликає посилену увагу бізнесу до проблем забезпечення власної економічної безпеки, які виходять на передній план не лише в кризових умовах функціонування економіки, але й при стабільному її розвитку [6].

В загальному розумінні з поняттям «економічна безпека підприємства» пов'язують здатність мобілізації та найбільш оптимального управління ресурсами підприємства з метою забезпечення його стабільного функціонування, активної протидії негативним впливам зовнішнього середовища. При цьому в умовах інформаційної ери – ери боротьби інформаційних технологій все більша увага приділяється вивченню ризиків, пов'язаних з інформацією, системами її обробки, відводячи визначальну роль інформаційній складовій забезпечення економічної безпеки підприємства.

Під інформаційною безпекою підприємства розуміють захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні.

Не зважаючи на те, що інформатизація викликала формування ряду беззаперечних переваг для суб'єктів підприємницької діяльності, проникнення інформаційних технологій у всі сфери діяльності підприємств призвело до виникнення ряду істотних проблем. Поширення комп'ютерних систем, об'єднання їх в комунікаційні мережі посилило можливість несанкціонованого проникнення в систему управління підприємством, що може не просто паралізувати роботу цілого підприємства, а й завдати значних матеріальних втрат. Сьогодні втрати лише банківського сектору в результаті комп'ютерних злочинів щорічно нараховують сотні мільярдів доларів, а звичайні підприємства не одноразово піддаються набігу рейдерських атак. Саме тому, забезпечення інформаційної безпеки

підприємства є невід'ємною частиною його економічної безпеки.

Як визначено законом України «Про інформацію» захисту підлягає інформація, володіння якою дає змогу її дійсному чи потенційному власнику одержати виграш моральний, матеріальний чи політичний [7].

Отже, на перший план виходить проблема захисту таких параметрів інформації як конфіденційність, цілісність, доступність, достовірність, погіршення яких може призвести до порушення систем управління технологічними процесами та достовірності фінансової документації, розголошенню комерційних таємниць та несанкціонованому доступу до персональних даних.

Під конфіденційністю інформації розуміють властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Цілісність. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації та видалення.

Достовірність - властивість інформації бути правильно сприйнятою, ймовірність відсутності помилок, безсумнівна вірність наведених відомостей, які сприймає людина.

Доступність - властивість інформаційного ресурсу, яка полягає в тому, що користувач, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки[8].

Як підтверджують дані світової статистики [9], втрата тільки 20% інформації викликає руйнацію 65% фірм та компаній, а погіршення її параметрів може призвести до вкрай тяжких наслідків, пов'язаних з розривом партнерських відносин, невиконання умов договорів, втратою вигідних контрактів, відмовою від прийнятих рішень, які стали не ефективними в результаті розголошення конфіденційної інформації. І як результат колосальні фінансові втрати компаній, які залишають свій відбиток не лише на обсягах виробництва та реалізації продукції, але й наносять «пляму» на авторитет та ділову репутацію компанії, призводячи в майбутньому в крайньому випадку або до повного банкрутства підприємства, або до більш жорстких умов отримання кредитів та труднощів в сфері співпраці з постачальниками.

При цьому за даними досліджень близько 75% витоку інформації компаній відбувається виключно за рахунок її розголошення співробітниками фірм, зі 100% опитаних працівників 25% завжди готові продавати комерційну таємницю [10].

В зв'язку з цим більшість підприємств вирішення проблем по забезпеченню власної економічної безпеки, пов'язують зі створенням сучасної корпоративної системи інформаційної безпеки, здатної сприяти захисту конфіденційності інформації від несанкціонованого доступу та нейтралізації факторів погроз економічній безпеці компанії.

На думку Волкова Я. така система повинна забезпечувати максимальне скорочення величини ризиків, пов'язаних з інформаційними технологіями, з мінімальним рівнем витрат на їх реалізацію та володіти високим запасом гнучкості для самостійної адаптації в умовах мінливого зовнішнього середовища [11].

На думку автора статті створення ефективної системи інформаційної безпеки підприємства вимагає розробки ряду юридичних, організаційно-економічних та технологічних заходів, спрямованих на:

- своєчасне виявлення та запобігання розголошенню конфіденційної інформації, аналіз причин та умов їх виникнення і реалізації;
- вивчення каналів розподілу інформації, виявлення та призупинення несанкціонованого доступу до них;
- розробку механізмів оперативного реагування на погрози, засновані на використанні різного роду юридичних, економічних, технічних засобів та методів їх виявлення і нейтралізації;
- організацію спеціальної системи документообігу, що виключає можливість несанкціонованого отримання інформації;
- попередження різного роду форм незаконного втручання в інформаційні ресурси підприємства, що створюють погрозу для підриву його економічної безпеки.

Однак, неперервний захист інформації можливий лише при створенні спеціальної системи захисту, побудованій з врахуванням індивідуальних особливостях кожного підприємства (організаційна структура, обсяг та характеристика інформаційних потоків, кількість та характер виконуваних операцій, функціональні обов'язки персоналу, характер клієнтів) та здатній забезпечувати комплексний характер захисту на всіх етапах життєвого циклу економічної системи.

Відповідно до цього організація та функціонування системи захисту інформаційної складової економічної безпеки підприємства повинні відповідати наступним принципам:

- Обґрунтованість. Засоби захисту інформаційних ресурсів, що використовуються на підприємств, повинні бути реалізовані на сучасному рівні розвитку науки і техніки, обґрунтовані з точки зору заданого рівня безпеки.
- Комплексність. Захист інформаційних ресурсів від можливих загроз повинен забезпечуватися всіма доступними законними засобами, методами і заходами на всіх технологічних

етапах обробки і використання інформації, у всіх режимах функціонування підприємства.

- Безперервність. Означає постійне підтримання всієї системи захисту в актуальному стані і вдосконалення її відповідно до мінливих умов функціонування підприємства.

- Спеціалізація. Експлуатація технічних засобів і реалізація системи заходів щодо забезпечення інформаційної безпеки повинно здійснюватися професійно підготовленими фахівцями.

- Взаємодія і координація. Комплекс заходів по забезпеченню захисту інформаційної складової економічної безпеки повинен проводитися на основі чіткого взаємозв'язку відповідних підрозділів і служб підприємства шляхом координації їх зусиль для досягнення поставлених цілей планом захисту.

- Вдосконалення. Передбачає розвиток заходів і засобів забезпечення інформаційної безпеки на основі власного досвіду, появи нових технічних засобів.

- Централізація управління. Означає управління інформаційною безпекою за єдиним організаційним, функціональним і методологічним принципам.

Останнім часом для забезпечення схоронності інформації підприємствами створюються цілі структурні підрозділи, які відповідають за збереження комерційних таємниць та забезпечення захисту від несанкціонованих втручань з боку зовнішнього оточення.

В цілому, як пропонує Ясенев В.М., основним етапами системи захисту інформації можна визначити[12]:

1. Аналіз можливих погроз. На цьому етапі визначається перелік реальних погроз, які можуть завдати серйозних збитків підприємству.

2. Розробка системи захисту (планування). Цей етап реалізації системи захисту інформації передбачає розробку комплексної системи захисту як сукупності засобів, здатних протидіяти впливам різного характеру. Результатом даного етапу є розробка плану захисту організації від несанкціонованих втручань, який містить перелік компонентів інформаційної системи підприємства, що підлягають захисту та можливий вплив на них, мету захисту інформації, правила її обробки та користування персоналом і користувачами інформаційної системи підприємства, детальний опис розробленої системи захисту.

Як правило, розроблений план захисту складається з пунктів, що характеризують політику безпеки, поточний стан системи, рекомендації по реалізації системи захисту, відповідальність персоналу, порядок введення в дію засобів захисту, дані про їх перегляд і склад.

3. На етапі реалізації системи захисту відбувається установка та настройка, визначених планом захисту, засобів захисту.

4. Етап супроводження системи захисту передбачає постійний контроль над роботою системи, реєстрацію подій, які відбуваються в ній, їх аналіз з метою виявлення факт порушення безпеки функціонування інформаційної системи підприємства.

В загальному вигляді етапність побудови системи захисту інформації підприємства можна представити у вигляді схеми(див. рис.1.).

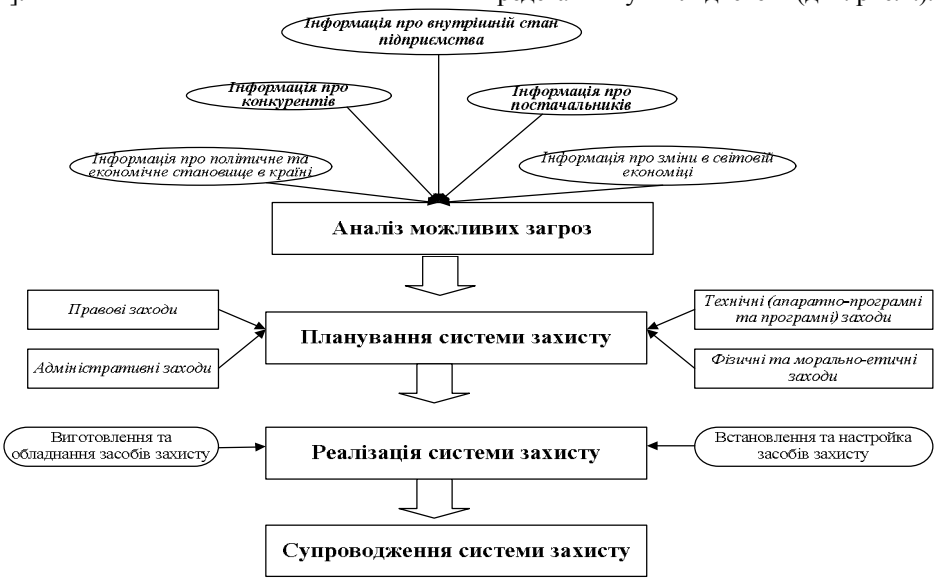

Рис. 1. Етапність побудови системи захисту інформації підприємства

У широкому розумінні підприємство володіє інформаційною безпекою якщо забезпечується не тільки надійність роботи комп'ютерних мереж, збереження цінних даних, захист інформації від несанкціонованого доступу та збереження таємниці переписки електронним зв'язком, але й виконуються основні принципи інформаційної безпеки підприємства, а саме:

принцип законності, невизначеності, мінімального ризику та мінімальної шкоди, безпечного часу, «захисту всіх від усіх», персональної відповідальності, обмеження повноважень, взаємодії та співпраці, комплексності та індивідуальності, послідовності рубежів безпеки тощо [12].

При цьому, більшість експертів та науковців, які цікавляться питанням інформаційного забезпечення економічної безпеки, відводять визначальну роль в її забезпеченні економіко-математичним методам [13] пошуку, збору, аналізу, обробки та використання інформації, які тим чи іншим чином сприяють підвищенню економічного потенціалу підприємства та передбачають оцінку важливості інформації, що потребує захисту, та інформаційних ризиків підприємства; оцінку вразливості інформації та системи, в якій вона функціонує та економічне обгрунтування доцільності витрат на забезпечення інформаційної безпеки.

Однак, розглядаючи зміст процесу забезпечення інформаційної складової економічної безпеки підприємства, необхідно зазначити, що будь-яка система повинна носити комплексний характер захисту та передбачати ряд заходів, здатних забезпечувати:

- постійний моніторинг каналів розподілу інформації, доступ працівників до інформаційних ресурсів підприємства з метою завчасно виявлення та попередження ймовірності її витоку за межі підприємства;
- постійний контроль інформації, що має характер комерційної таємниці підприємства з метою передбачення можливостей незаконного втручання на всіх рівнях обробки даних та можуть призвести до її знищення, руйнування, спотворення;
- організацію безвідмовної роботи інформаційних систем та ресурсів підприємства;
- прогнозування тенденцій розвитку наукового та технологічного потенціалів підприємства з метою встановлення можливості факту незаконного заволодіння об'єктами інтелектуальної власності компанії;
- реалізацію, передбачених планом захисту, рекомендацій для забезпечення стабільного рівня економічної безпеки за всіма її складовими тощо.

Висновок. Таким чином, інформаційна складова економічної безпеки підприємства в системі випереджаючого розвитку інформаційних технологій виступає основним фактором забезпечення захищеності інформаційних ресурсів компанії та важливим чинником стабільного функціонування підприємств, ефективна реалізація якого сприятиме не тільки збереженню комерційних таємниць, але й дозволить попередити можливості непередбачуваних фінансових втрат.

СПИСОК ЛІТЕРАТУРИ

1. Донець Л.І. Економічна безпека підприємства [Текст]: навч. пос. / Л.І. Донець, Н.В. Ващенко. –К.: Центр учбової літератури, 2008. – 240 с.
2. Мунтіян В.І. Економічна безпека України [Текст] /В.І. Мунтіян. – К.: КВІУ, 1999. – 464 с.
3. Козаченко Г.В. Економічна безпека підприємства: сутність та механізм забезпечення [Текст]: Монографія / Г.В.Козаченко, В.П. Пономарьов, О.М.Ляшенко. – К.: Лібра, 2003. – 280 с.
4. Пастернак-Таранушенко Г. А. Економічна безпека держави. Статика процесу забезпечення [Текст] / Г. Пастернак-Таранушенко; за ред. проф. Б. Кравченка. – К. : Кондор, 2002. – 302 с.
5. Шлемко В.Т Економічна безпека України: сутність і напрямки забезпечення [Текст]: монографія / В. Т. Шлемко, І. Ф. Бінько. – К.: НІСД. – 1997. – 144 с.
6. Тишаев В.В. Информационная составляющая экономической безопасности хозяйствующих субъектов и ее значение для обеспечения устойчивого развития национальной экономики [Текст] / В.В. Тишаев// Управление общественными и экономическими системами, 2007. - №.1. – С.1-11.
7. Закон України «Про інформацію» [Електронний ресурс]. Режим доступу: http://zakon1.rada.gov.ua/laws/show/2657-12.
8. Богуш В.М. «Інформаційна безпека [Текст]: Термінологічний навчальний довідник» / В. М. Богуш, В. Г.Кривуца, А. М. Кудін; За ред. Кривуцої В. Г. — Київ, 2004. — 508 с
9. Прокоф'єва Д.М. Підприємницьке шпигунство в системі інформаційних злочинів [Текст] / Д.М. Прокоф'єва // Український центр інформаційної безпеки. 2008. – С.123-128.
10. Ткачук Т. Формування системи інформаційної безпеки бізнесу [Текст] / Т.Ткачук // Бізнес і безпека, 2009. - №4. – С.19-23.
11. Волков Я. Системы обеспечения информационной безопасности как часть корпоративной культуры современной организации [Текст] / Я.Волков // Финансовая газета, 2006. – №34. – С.15.
12. Ясенев В.Н. Информационная безопасность в экономических системах [Текст]: Учебн.пособ /В.Н. Ясенев. – Новгород: Изд-воННГУ, 2006. – 253 с.
13. Гриджук Г.С. Систематизація методів інформаційної безпеки підприємства [Електронний

ресурс] /Г.С.Гриджук. Режим доступу: 1/pdf/64.pdf13. http://www.nbuv.gov.ua/portal/natural/vntu/2009_19_

Аннотация. В статье раскрыты принципы функционирования системы информационной безопасности предприятия и исследовано этапность создания системы защиты информационных ресурсов предприятия.

Ключевые слова: экономическая безопасность, информационные ресурсы, предприятие.

Summary. In the article the principles of information security system company and investigated phasing creation of information resources protection company.

Keywords: economic security, information resources company.

Рецензент *к.е.н., доцент УкрДАЗТ Якименко Н.В.*
Експерт редакційної колегії *к.е.н., доцент УкрДАЗТ Сухорукова Т.Г.*

УДК 338.5:656.611.2

ЗАСАДИ АДАПТАЦІЇ СИСТЕМ РОЗВИТКУ ПЕРСОНАЛУ ПОРТОВИХ ПІДПРИЄМСТВ ДО СУЧАСНИХ УМОВ

Наконечний Ю.В., аспірант (ОНМУ)

У статті розкрито сутність та основні підходи адаптації систем розвитку персоналу портових підприємств до сучасних умов . Обгрунтовано доцільність та особливості процесу формування мотиваційного поля портових підприємств. Дана характеристика зовнішньої та внутрішньої складових мотиваційного поля портових підприємств.

Ключові слова**: **трудові ресурси, розвиток персоналу, мотиваційне поле, підприємство портової діяльності.

Постановка проблеми. Висока інтенсивність конкуренції на ринках портової продукції (робіт, послуг), висока мінливість зовнішнього середовища спонукає вітчизняні підприємства портової діяльності виявляти резерви підвищення конкурентоспроможності. Найважливішою передумовою утримання та покращення конкурентних позицій є розвиток персоналу.

У світовій портовій діяльності завдяки використанню цільового капіталу та різних форм приватно-державного партнерства реалізуються масштабні національні та регіональні інвестиційні проекти в сфері портової діяльності, забезпечується розвиток персоналу, що дозволяє ефективно взаємодіяти із клієнтурою, партнерами, іншими економічними суб'єктами.

В процесі розвитку трудового потенціалу портових підприємств головним завданням є забезпечення відповідності його кваліфікації сучасним умовам функціонування організації. Задля забезпечення інноваційного розвитку портового підприємства персоналу обов'язково мають бути притаманні такі характеристики: володіння навичками концептуального мислення, готовність до змін, висока працездатність і адекватне розуміння перспектив розвитку, готовність концентруватися в короткі терміни заради досягнення цілей, готовність до роботи з нечіткими межами і розмиванням функцій, вміння орієнтуватися в системі шляхів розв'язання проблем. Відповідно необхідно створити механізми, які будуть зв'язувати стратегічний розвиток підприємства з розвитком його людських ресурсів. Існують ідеї перетворення портових підприємств на самонавчальні організації.

Огляд останніх досліджень і публікацій. Існують численні публікації, що віддзеркалюють результати досліджень в сфері формування трудового потенціалу на рівні держави, регіонів та окремих суб'єктів господарювання. Так В.В. Онікієнко, Л.Г. Ткаченко, Л.М. Ємельяненко дослідили особливості розвитку ринку праці України та визначили його перспективи [3]. Багато уваги приділено проблемам управління людськими ресурсами [5, 7]. Вчені виконували спроби з різних точок зору оцінювати трудовий потенціал на рівні підприємства [6].

Невирішені складові загальної проблеми. Однак, у літературних джерелах, що присвячені проблемам формування напрямків розвитку трудових ресурсів, не в повному обсязі розглядаються ефективні підходи щодо адаптації систем розвитку персоналу до умов, що постійно змінюються. Крім того, важливими є визначення основ різноманітних підходів та розробка механізму їхньої адаптації до умов функціонування конкретних підприємств, зокрема морських портів. Багато проблем існує в сфері теоретичного забезпечення практичної реалізації мотиваційних систем транспортних підприємств, зокрема морських торговельних портів [2, 4]. Проте, останнім часом швидко розвиваються