Проблеми забезпечення інформаційної складової економічної безпеки сучасних підприємств

Орлик О.В.
кандидат економічних наук
доцент кафедри економічної кібернетики та інформаційних технологій
Одеського національного економічного університету

Сучасні умови господарювання, що характеризуються високим рівнем нестабільності зовнішнього та внутрішнього середовища, свідчать, що розвиток економіки і бізнесу неможливий без забезпечення інформаційної складової економічної безпеки та активної протидії кіберзлочинності.

Вітчизняні підприємства змушені будувати стратегію власного розвитку та виживання, засновану на широкому застосуванні інформаційних технологій. Однак, тільки невелика кількість підприємств виділяють на забезпечення інформаційної складової економічної безпеки достатні обсяги коштів для запобігання, локалізації та усунення різних видів загроз.

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. Інформаційні технології розширили можливості підприємств, забезпечили прискорення процесів обміну та співпраці, відкрили доступ до більш ефективних методів управління, однак й створили умови для підриву власної економічної безпеки підприємств, зниження рівня стабільності їх фінансово-економічної діяльності [1, с. 250].

З розвитком комп'ютерних інформаційних технологій загострилася проблема комп'ютерних злочинів, які можуть завдати підприємству як фінансових, так і інформаційних втрат [2, с. 169].

Підприємства при виконанні своїх функцій отримують через різні інформаційні канали значну кількість інформації, що формує різні механізми кіберзлочинності: Інтернет-шахрайство; розкрадання грошових коштів; розповсюдження комп'ютерних вірусів; атаки в Мережі та ін.

Можливість зовнішнього і внутрішнього втручання в інформаційну систему підприємства впливає на викривлення таких параметрів інформації, як конфіденційність, цілісність, доступність, достовірність та ін.

Це може привести до негативних наслідків у діяльності підприємства: збоїв у функціонуванні систем управління технологічними та управлінськими процесами; розголошення відомостей, що становлять комерційну та інші види таємниць; порушення достовірності фінансової звітності; несанкціонованого доступу до бази даних підприємства; викривлення публічної інформації тощо.

Результатом викривлення інформації про діяльність підприємства можуть стати: зменшення вартості капіталу підприємства; труднощі залучення інвестицій; розрив (або погіршення) ділових відносин із партнерами; зрив переговорів, втрата вигідних контрактів; невиконання договірних зобов'язань; відмова від рішень, які стали неефективними через розголос інформації; втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію; зниження цін або обсягів реалізації; нанесення шкоди авторитету та діловій репутації підприємства; більш жорсткі умови отримання кредитів; труднощі в постачанні та придбанні устаткування тощо [3, с. 139].

У широкому розумінні підприємство володіє інформаційною безпекою, якщо забезпечується надійність роботи комп'ютерних мереж, збереження цілісності даних, захист інформації від несанкціонованого доступу, збереження таємниці переписки електронним зв'язком.

Незважаючи на ряд беззаперечних переваг, 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.

Захист інформації можливий лише при створенні спеціальної системи захисту, побудованій з урахуванням індивідуальних особливостей кожного підприємства, здатній забезпечувати комплексний захист, повністю відповідати специфіці діяльності підприємства, працювати гармонічно з основними процесами і реагувати на всі сигнали, що від них надходять.

Така система захисту повинна забезпечувати скорочення рівня ризиків, пов'язаних із застосуванням інформаційних технологій, бути гнучкою для адаптації в умовах мінливого зовнішнього середовища.

Створення ефективної системи інформаційної безпеки підприємства вимагає розробки ряду 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 загрози, 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 загрозу для підриву його економічної безпеки [1, с. 251].

Останнім часом, для забезпечення інформаційної складової економічної безпеки, підприємства створюють структурні підрозділи, які відповідають за збереження комерційних таємниць та забезпечення захисту від несанкціонованих втручань з боку зовнішнього оточення. При цьому повинні виконуватися основні принципи інформаційної безпеки, а саме: законності; обґрунтованості; комплексності; безперервності; взаємодії і координації; вдосконалення; мінімального ризику та мінімальної шкоди; безпечного часу; персональної відповідальності; обмеження повноважень; послідовності рубежів безпеки тощо.

В цілому можна виділити такі основні етапи розробки системи захисту інформації на підприємствах: аналіз можливих загроз; розробка (планування) системи захисту; реалізація системи захисту; супроводження системи захисту [1, с. 252].

На етапі аналізу можливих загроз визначається перелік реальних загроз, які можуть завдати серйозних збитків підприємству, на основі інформації про: внутрішній стан підприємства, конкурентів, постачальників, політичне та економічне становище в країні, зміни в світовій економіці тощо.

Етап планування системи захисту передбачає розробку комплексної системи захисту як сукупності засобів, здатних протидіяти впливам різного характеру. Результатом даного етапу є розробка плану захисту організації від несанкціонованого втручання, 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.

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

Супроводження системи захисту передбачає постійний контроль над процесами системи, реєстрацію подій, які відбуваються в ній, їх аналіз з метою виявлення фактів порушення безпеки функціонування інформаційної системи.

Забезпечення інформаційної безпеки в загальній постановці проблеми може бути досягнуте лише при взаємопов'язаному розв'язку трьох складових:

– захисту інформації, що перебуває в системі, від дестабілізуючого впливу зовнішніх і внутрішніх загроз;

– захисту елементів системи від дестабілізуючого впливу зовнішніх і внутрішніх інформаційних загроз;

– захисту зовнішнього середовища від інформаційних загроз з боку самої системи [4].

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 з метою завчасного 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; 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 рекомендацій, передбачених планом захисту, для забезпечення стабільного рівня економічної безпеки за всіма її складовими тощо [1, с. 253].

Таким чином, забезпечення інформаційної безпеки підприємства є невід'ємною частиною його економічної безпеки. Інформаційна складова економічної безпеки підприємства виступає основним фактором забезпечення захищеності його інформаційних ресурсів та важливим чинником стабільного функціонування підприємства.

Література:

1. Міщенко С. П. Інформаційна складова економічної безпеки підприємства // Вісник економіки транспорту і промисловості. 2012. № 39. С. 250–254.

2. Орлик О. В. Інформаційні технології забезпечення безпеки електронного бізнесу // Кібербезпека в Україні: правові та організаційні питання: матеріали Всеукр. наук.-практ. конф., м. Одеса, 21.10.2016 р. Одеса: ОДУВС, 2016. - С. 167–169.

3. Нехай В. А. Інформаційна безпека як складова економічної безпеки підприємств // Науковий вісник Міжнародного гуманітарного університету. Серія: «Економіка і менеджмент». 2017. Вип. №24. Ч. 2. С. 137–140.

4. Філімонюк К. С., Тарасенко І. О. Управління захистом інформації в системі фінансово-економічної безпеки підприємства. URL: https://www.inter-nauka.com/uploads/public/14490531775333.pdf (дата звернення: 13.11.2018).