УДК 330.115:658.1

Куркін Н.В.

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ СУЧАСНОГО РОЗВИТКУ ПІДПРИЄМСТВА

Питанням забезпечення економічної безпеки держави, регіонів і підприємств присвячена ціла низка робіт вітчизняних учених і практиків [1,3,4,8,10]. Їх вивчення дозволило визначити певні етапи в розвитку цього напрямку організаційно-управлінської діяльності підприємств та дійти висновку, що в них адекватно досліджувались стан справ та задачі, що стояли в галузі забезпечення безпеки на кожному з цих етапів та пропонувалися відповідні шляхи такого забезпечення.

Так, на першому етапі проблема, в основному, зводилася до збереження й захисту комерційної таємниці та інших секретів підприємства. На наступному етапі акцент проблеми безпеки діяльності суб'єктів господарювання був перенесений на організацію захисту від впливу зовнішнього середовища й пристосування (адаптацію) до його стану. Низка сучасних дослідників дотримується ресурсно-функціонального підходу до забезпечення економічної безпеки підприємств, розглядаючи її як стан найбільш ефективного використання корпоративних ресурсів для запобігання загроз та забезпечення стабільного функціонування в даний час і у майбутньому.

У сучасних наукових виданнях, присвячених проблемам безпеки функціонування бізнес-структур, значне місце приділяється проблемі захисту інформації й кадрів (персоналу) [3,8,10]. Причому останні характеризуються як особливий фактор - джерело розголошення комерційної таємниці. В свою чергу, інформація й розширення комунікативних зв'язків підприємства - це особливий аспект проблеми організації економічної безпеки діяльності підприємств, який набуває всезростаючого значення.

Зміна етапів дослідження проблеми, розширення кола завдань, що стоять в цьому напрямку перед підприємствами, пов’язані з головною об'єктивною історичною характеристикою соціально-економічних систем - закономірністю безперервного розвитку й відтворення їх ресурсно-функціонального потенціалу.

З одного боку розвиток є іманентною характеристикою виробництва, умовою завоювання конкурентної позиції підприємства, значення якої посилюється в зв’язку з ускладненням конкурентного середовища, з іншого, - розвиток, як загальний принцип існування природи, суспільства й пізнання, будучи об'єктивним процесом, супроводжується переходом предмета розвитку в сферу невизначеності, де закономірно формується система загроз, що, в свою чергу, є вагомою підставою комплексного та з випередженням вирішення завдань по забезпеченню безпеки ресурсного потенціалу, у тому числі його організаційно-структурних характеристик.

Серед об'єктів, що входять у систему обмінних комунікативних зв'язків підприємства в процесі розвитку виробничо-господарської діяльності й формують його загрози, зростаючого значення набувають потоки інформації, які несуть в собі стратегічні відомості про рух всіх видів ресурсів, інвестиції й фінансування, поставки товарно-матеріальних цінностей, придбання нових технологій, патентів, ліцензій, залучення кваліфікованого персоналу тощо [2].

Особлива увага приділяється інформаційній безпеці, яка реалізує різні схеми захисту інформації з погляду таких властивостей інформації, як цілісність, системність, доступність і конфіденційність, що знайшло своє підтвердження в роботах [3, 5, 9]. Врахування цих характеристик дозволяє сформулювати безпечні режими роботи з інформацією і визначає ефективність засобів захищеності інформаційних ресурсів інформаційної системи, що експлуатується на підприємстві. При цьому дослідники застосовують відомі моделі «порушників» [6], а також моделі захисту окремих підсистем (компонент) інформаційної системи підприємства. Моделі «порушників» включають як об'єкти загроз, так і їхні суб'єкти, що впливають на різні інформаційної системи і персонал з метою нанесення їм збитку. При цьому рівень інформаційної безпеки інтерпретується як рівень регламентного забезпечення безпеки таких об'єктів як програмні засоби, засоби, що забезпечують доступ до даних, права користувачів щодо виконання робіт, пов'язаних з модифікацією й використанням конфіденційної інформації, виявлення і протидії витоку інформації, стосовно виникаючих загроз, носіями яких виступають суб'єкти.

 ISSN 1562-9945

Використання системного підходу до організації процесів забезпечення інформаційної безпеки підприємства на основі положень теорії інформації, уточнення поняття інформаційного ресурсу та визначення інформаційної системи як підтримуючої системи відносно інформаційних ресурсів - найважливіше завдання підвищення ефективності інформаційної безпеки підприємства.

Для проведення дослідження на основі цього підходу розглянемо наступні поняття й визначення інформації.

Під інформацією звичайно розуміється множина даних, кожна підмножина яких характеризується такими властивостями, як об'єктивність, вірогідність, адекватність, своєчасність, коректність, точність, корисність, цінність. В різних літературних джерелах із зазначеної множини властивостей виділяють тільки певну частину з них, керуючись, у першу чергу, винятково практичними міркуваннями. Так, наприклад, властивості адекватності й вірогідності об'єднують в одну – вірогідності; об'єктивності й коректності – у властивість об'єктивності й т.д. Проаналізуємо решту властивостей – своєчасність, точність, корисність і цінність. Очевидним є той факт, що визначальною є властивість корисності, яка свідчить, що інформація повинна бути точною та своєчасною. Таким чином, можна висловити базове положення, що властивість інформації, визначальною мірою, характеризує певну функцію управління, реалізовану суб'єктом, який використовує інформацію.

Інформація, що використовується суб'єктом відносно якої-небудь дії, повинна реалізувати/виконувати певну функцію суб'єкта в системі/ структурі управління підприємством. В якості таких функції можна розглядати функції управління виробництвом, прийняття рішень, планування й т.д.

В наслідок того, що реалізована функція управління визначається рівнем управління і відповідних функцій суб'єкта управління, можна припустити, що потреба в інформації, у першу чергу, визначається тією її властивістю (або ж сукупністю властивостей), яка вважається основною у процесі її використання.

Для ефективної реалізації своєї управлінської функції суб'єктові необхідно розвивати кількісні і якісні характеристики тієї властивості, яка є основною, обов'язковою, такою, що часто використовується (або ж групи властивостей).

Таким чином, безпека розвитку інформаційних ресурсів визначається безпекою розвитку тих властивостей інформації, які є визначальними для суб'єкта; рівнем управління; характером розв'язуваних завдань; і, як наслідок, змістом посадових інструкцій; існуючою схемою документообігу.

Вищезазначене передбачає використання нової концепції інформаційної безпеки, основні положення якої є такі:

1) розвиток інформаційних ресурсів розглядається як сукупність процесів, процедур, окремих операцій, що забезпечують розвиток різних властивостей інформації;

2) безліч властивостей інформації визначається рівнем управління й, відповідно, тими завданнями, які, в першу чергу, вирішуються суб'єктом у процесі його діяльності з досягнення цілей;

3) безпека інформаційних ресурсів визначається рівнем управління й безпекою розвитку тих властивостей інформації, які є базовими для даного рівня управління підприємством;

4) безпека інформаційної системи визначається безпекою функціонування її підсистем і компонентів, які забезпечують конфіденційність, цілісність, доступність інформації на всіх рівнях управління підприємством;

5) основна функція інформаційної системи - забезпечення (забезпечувальна підсистема) безпечного розвитку властивостей інформації на всіх рівнях управління підприємством.

Отже, інформаційна система виступає як комплексний інструментальний засіб (сукупність засобів), який забезпечує безпечний розвиток властивостей інформаційних ресурсів на всіх рівнях управління підприємством.

Для реалізації цих концептуальних положень в системі інформаційної безпеки підприємства необхідно вирішити такі першочергові завдання: розподіл завдань між персоналом, технічними засобами, адміністраторами підсистем інформаційної системи; розробку інструкцій, нормативних матеріалів, у яких встановлюються гранично припустимі рівні, що відповідають вимогам категорій безпеки; визначення мінімально припустимої конфігурації програмно-апаратних засобів, які відповідають вимогам, що висуваються до інформаційної системи та забезпечують мінімальний

 ISSN 1562-9945

рівень потенційного збитку, що може бути нанесений підприємству; забезпечення захисту самої інформаційної системи.

Реалізація цих заходів щодо інформаційної безпеки дозволяє деталізувати її до різних рівнів управління підприємством, внести зміни в посадові інструкції осіб, які мають відношення до конфіденційної інформації і спроектувати можливі рівні захисту для різних видів загроз, що мають місце в зовнішньому і внутрішньому середовищах підприємства. Подальший напрямок досліджень пов'язаний з деталізацією запропонованої моделі відносно описаних категорій захисту, властивостей інформаційних ресурсів, що розвиваються, моделей захисту інформаційної системи в цілому і її окремих компонентів.

В аспекті розвитку економічних відносин важливе місце займають інформаційні системи підприємств, що виступають як інформаційний компонент системи управління підприємством. Подання інформаційної системи у вигляді сукупності власно даних, інформації та різних продуктів, породжених нею, методів і засобів її організації, зберігання, а також маніпулювання ними, обробки, аналізу, підходів до вироблення управлінських рішень вимагає розробки методик підвищення стабільності інформаційної системи підприємства в двох аспектах: стабільності протікання процесів, стабільності функціонування програмно-апаратних засобів і психологічної стабільності персоналу.

З погляду інформаційної безпеки, підвищення стабільності інформаційної системи може розглядатися як мінімізація ризиків спричинення збитків її підсистемам, компонентам та елементам у результаті навмисних або ненавмисних дій з боку суб'єктів (внутрішніх і зовнішніх), які беруть участь у процесах, що відбуваються в інформаційній системі, або ж запобігання завданню збитків за рахунок розробки і проведення відповідних заходів щодо захисту всіх елементів і процесів, які забезпечують функціонування інформаційної системи.

Аналіз досліджень у цій сфері показав, що на даний момент відсутній комплексний підхід до забезпечення безпеки інформаційної системи: так, наприклад, деякі автори розглядають інформаційну систему як сукупність елементів інформаційної інфраструктури, причому з метою забезпечення її безпеки для кожного з елементів

розробляються своя модель, методи й засоби захисту [3]. Цей підхід відрізняється тим, що інформаційна інфраструктура характеризується безліччю процесів, які безпосередньо відносяться до формування і обробки інформації, комунікаційними зв'язками (відносинами) з елементами організаційної структури, персоналом, різними суб'єктами, що використовують інформацію, і т.ін. [3]. Ці елементи самі є джерелами інформації на підприємстві, що, в свою чергу, призводить до значного збільшення її обсягу, складності і вимагає впорядкованості для підвищення рівня задоволення нею потреб користувачів. У зв'язку із цим виникає проблема фільтрації так називаного «інформаційного шуму» - інформації і відомостей, які є надлишковими, неактуальними, різнорідними, такими, що перешкоджають використанню інформації, яка є найбільш релевантною для вирішення проблеми або задачі в сформованій ситуації.

Іншим завданням є розробка методів підвищення стабільності інформаційної системи підприємства на основі мінімізації ризиків, пов'язаних із завданням збитків як діяльності підприємства, так і його інформаційній інфраструктурі та підвищення стабільності всіх інформаційних процесів, включаючи методи і засоби одержання, введення, обробки та аналізу інформації.

Для вирішення цього завдання сформулюємо наступні положення, які лежать в основі методу забезпечення інформаційної стабільності на підприємстві:

- об'єктами забезпечення інформаційної стабільності є інформаційні процеси, інформаційні продукти, отримані в процесах перетворення інформації, та інформаційна інфраструктура підприємства в цілому;

– стабільність інформаційних процесів визначається збереженням всіх властивостей інформації й інформаційних продуктів, створених у процесі життєвого циклу інформаційних продуктів;

– життєвий цикл інформаційних продуктів характеризується часовим обмеженням, тривалість якого визначається тривалістю етапів їхнього формування, становлення й розвитку;

 ISSN 1562-9945

- безпека і підвищення стабільності інформаційного продукту забезпечується сукупністю засобів захисту на всіх етапах його життєвого циклу;

– засоби захисту існуючої інформаційної інфраструктури підприємства базуються на засобах захисту, що використовуються у тих процесах, які пов'язані зі зберіганням, введенням, модифікацією і передачею інформації за умови збереження всіх її властивостей;

– засоби захисту забезпечують захист інформаційного продукту на всіх етапах його життєвого циклу.

Таким чином, інформаційна складова набуває зростаючого значення і виступає як комплексний інструментальний засіб у забезпеченні безпечного розвитку підприємства. Концепція інформаційної безпеки повинна базуватися на наявному стані і реальній оцінці місця інформаційниї ресусів та потреб інформаційного забезпечення розвитку підприємства, корегуватися в зв’язку зі змінами цих параметрів та бути основою для розробки методичних підходів до забезпечення інформаційної стабільності на підприємстві.

ЛІТЕРАТУРА

1. Андрощук Г. А. Экономическая безопасность предприятия: защита комерческой тайны: Монография / Г. А. Андрощук, П. П. Крайнев. – К.: Изд. дом "Ин Юре", 2000. – 400 с.
2. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
3. Економічна безпека підприємства: сутність та механізм забезпечення: Монографія / Г. Б. Козаченко, В. П. Дономарьов, О. М. Ляшенко. – К.: Лібра, 2003. – 280 с.
4. Мунтіян В. І. Глобалізація інвестиційних процесів та економічна безпека України // Фондова панорама. – 2005. – № 49. – С. 1-2.
5. Организация и современные методы защиты информации / Под общ. ред. Диева С. А., Шаваева А. Г. – М.: Банковский деловой центр, 1998. – 472 с.
6. Петренко С. А. Возможная методика построения системы информационной безопасности предприятия // Прогноз финансовых рисков / www.bre.ru.
7. Соколов А. В. Как оценить угрозы безопасности информации? // Элвис + / http://www.elvisplus.ru.
8. Тридід О. М. Організаційно-економічній механізм стратегічного розвитку підприємства: Монографія. – Харків: Вид. ХДЕУ, 2002. – 364 с.

9. Устинов Г. Н. Основы информационной безопасности систем и сетей передачи данных. – М.: СИНТЕГ, 2000. – 248 с.
10. Черняк О. І. Моделювання економічної безпеки на макро- і мезорівнях. В кн.: Моделювання економічної безпеки: держави, регіону, підприємства // Монографія. – Харків: ВД «ІНЖЕК», 2006. – 240 с.

Получено 26.03.07 г.

 ISSN 1562-9945