УДК 658.012.2

МЕТОДОЛОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

METHODOLOGICAL ASPECTS OF INFORMATION SECURITY OF THE ENTERPRISE

Фісуненко П.А.
кандидат економічних наук, доцент,
доцент кафедри економіки та підприємництва,
Придніпровська державна академія будівництва та архітектури

Судакова О.І.
кандидат технічних наук, доцент,
доцент кафедри економіки та підприємництва,
Придніпровська державна академія будівництва та архітектури

Деркач С.В.
магістр,
Придніпровська державна академія будівництва та архітектури

Притуляк Є.О.
магістр,
Придніпровська державна академія будівництва та архітектури

Fisunenko Pavel
Candidate of Economic Sciences, Associate Professor,
Associate Professor, Department of Economics and Entrepreneurship,
Pridneprovsk State Academy of Civil Engineering and Architecture

Sudakova Oksana
Candidate of Technical Sciences, Associate Professor,
Associate Professor, Department of Economics and Entrepreneurship,
Pridneprovsk State Academy of Civil Engineering and Architecture

Derkach Stanislav
magister,
Pridneprovsk State Academy of Civil Engineering and Architecture

Pritulyak Evgeniy
magister,
Pridneprovsk State Academy of Civil Engineering and Architecture

Статтю присвячено актуальним питанням забезпечення інформаційної безпеки у стратегіях розвитку підприємства. 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. Наведено систематизовану класифікацію загроз інформаційній безпеці. Виділено властивості інформації, які в першу чергу визначають рівень її захищеності, визначаються суб'єктами, що провадять цю інформацію, а також виробленими ними інформаційними продуктами і послугами. Обґрунтовано, що механізми протидії інформаційній зброї повинні базуватися на посиленні позитивних чинників – інформаційної інфраструктури і зменшенні (нейтралізації) негативних чинників, перепрограмуванні інформаційної інфраструктури на основі таких дестабілізуючих дій, як навмисна модифікація та інтерпретація інформаційних продуктів й їхніх похідних, із метою виділення таких процедур, технологій маніпулювання ними, які б дали змогу досягти переваги в матеріальній сфері. Пропонується підрозділяти протидії за

пасивним (нейтралізуючим) і активним характером. Визначено, вирішення яких завдань може містити в собі пасивні та активні протидії.

Ключові слова: *інформаційна безпека підприємства, інформація, загрози інформаційній безпеці, пасивні протидії, активні протидії, дестабілізуючі дії, інформаційні продукти, інформаційні послуги, інформаційна система, розвиток підприємства.*

Статья посвящена актуальным вопросам обеспечения информационной безопасности в стратегиях развития предприятия. Использование системного подхода к организации процессов обеспечения информационной безопасности предприятия на основе положений теории информации, уточнение понятия информационного ресурса и определения информационной системы в качестве поддерживающей системы относительно информационных ресурсов – важнейшая задача повышения эффективности информационной безопасности предприятия. Приведена систематизированная классификация угроз информационной безопасности. Выделены свойства информации, которые в первую очередь определяют уровень ее защищенности, определяются субъектами, которые осуществляют эту информацию, а также производимыми ими информационными продуктами и услугами. Обосновано, что механизмы противодействия информационному оружию должны базироваться на усилении позитивных факторов – информационной инфраструктуры и уменьшении (нейтрализации) негативных факторов, перепрограммировании информационной инфраструктуры на основе таких дестабилизирующих действий, как умышленная модификация и интерпретация информационных продуктов и их производных, с целью выделения таких процедур, технологий манипулирования ими, которые позволили бы достичь преимущества в материальной сфере. Предлагается подразделять противодействия за пассивным (нейтрализующим) и активным характером. Определено, решения каких задач могут включать в себя пассивные и активные противодействия.

Ключевые слова: *информационная безопасность предприятия, информация, угрозы информационной безопасности, пассивные противодействия, активные противодействия, дестабилизирующие действия, информационные продукты, информационные услуги, информационная система, развитие предприятия.*

Methodological aspects of organizing an effective enterprise security system and managing it include ensuring the security of its resources – financial, material, information, labor – and the safety of their interaction with objects related to the internal and external environments of the enterprise. Nowadays actual problems are connected with integration of Ukraine into the world economic system and their decision is accompanied by various integration and the globalization processes. Openness of the world community also requires openness of Ukraine one of the factors of which is the information aspect. The article focuses on topical issues of information security in the enterprise development strategies. It is proposed to use a systematic approach to the organization of processes of ensuring information security of the enterprise based on the provisions of the theory of information, clarifying the concept of information resource and defining the information system as a support system for information resources – the most important task of improving the efficiency of information security of the enterprise. The systematic classification of information security threats is presented. The properties of information, which first of all determine the level of its security, are determined by the entities that produce this information, as well as the information products and services produced by them. It is substantiated that mechanisms of counteraction to information weapons should be based on strengthening of positive factors – information infrastructure and reduction (neutralization) of negative factors, reprogramming of information infrastructure on the basis of such destabilizing actions as deliberate modification and interpretation of information products and their methods of derivation manipulating them that would allow them to achieve material advantages. It is proposed to divide the counteraction by passive (neutralizing) and active nature. This solution of tasks can include passive and active counteraction. Presented by the formation of the enterprise mechanisms, combined with the mechanisms of manifestation of factors of information security and security of resources of the enterprise as a whole, will allow to form stable modes of functioning of the information system and improve the quality of the managed development of the enterprise.

Key words: *information security of the enterprise, information, threats to information security, passive counteraction, active counteraction, destabilizing actions, information products, information services, information system, enterprise development.*

Постановка проблеми у загальному вигляді та її зв'язок із важливиминауковими чи практичними завданнями. Прихованість багатьох інформаційних впливів має не останнє значення під час застосування інформаційної зброї. Скоріше за все, найважливішим у всій цій історії є те, що жертви даного виду зброї, навіть володіючи теорією і відповідною матеріально-технічною базою, приходять до усвідомлення себе як жертви тільки потім, коли вже нічого не можна змінити. Таким чином, необхідно виходити з того, що в епоху інформаційних технологій, коли соціальне середовище перенасичене інформацією, безпека інформаційної системи визначаються не тільки тими знаннями про супротивника, які дана система одержує, а й, напевно, передусім тими знаннями, від сприйняття яких їй удалося ухилитися. Тому в умовах

загострення економічної кризи, що поставила на межу виживання низку підприємств, які ще донедавна вважалися успішними й стабільно функціонуючими, питання про інформаційну безпеку набуло особливої актуальності.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спираються автори. Сьогодні в науковій літературі значна увага приділяється питанню інформаційної безпеки підприємств. Вагомий внесок у дослідження, пов'язані з проблемами інформаційної безпеки, зробили такі вітчизняні і зарубіжні науковці: Н.С. Безугла, О.Р. Бойкевич, Т.Г. Васильців, Г.Б. Веретенникова, О.А. Грунін, С.О. Грунін, Я.А. Жаліло, А.В. Іванов, Г.Б. Клейнер, Г.В. Козаченко, Т.Б. Кузенко, В.А. Ліпкан, В.Я. Пригунов, А.С. Соснін, А.Г. Шаваєв, В.В. Шликов, В.І. Ярочкін, В.М. Ячменьова та ін. [1–4]. Дослідження вітчизняних та зарубіжних учених показують, що для підприємства більш важливим є не уникнення загрози взагалі, а вміння вчасно і точно її передбачити, щоб ужити необхідних заходів. Це стосується як підприємств, що знаходяться у кризовому стані, так і успішно працюючих підприємств.

Виділення не вирішених раніше частин загальної проблеми, котримприсвячується означена стаття. Однак залишилася невирішена проблема – недостатньо розкрито проблеми застосування інформаційної системи та впровадження її до механізму управління економічною безпекою підприємства.

Формулювання цілей статті **(постановка завдання)**. Метою статті є розроблення методологічних аспектів забезпечення інформаційної безпеки підприємства в умовах нестабільного економічного середовища на основі застосування інформаційної системи та впровадження її до механізму управління економічною безпекою підприємства.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Інформаційна безпека є основою безпеки сучасних відкритих суспільних систем і, своєю чергою, ґрунтується на політиці інформатизації й інформаційному аспекті політики економічної безпеки держави як сукупності суспільних систем. До основних напрямів інформатизації суспільства в Україні, згідно з чинними на поточний момент документами нормативного і правового забезпечення, належать державна політика у сфері інформатизації і державна політика у сфері економічної безпеки. Виходить, що вирішення завдань, пов'язаних із проблемами інформатизації та економічної безпеки, інтегрується в єдину систему інформаційної безпеки.

Розглянемо аспекти, що синтезують зазначені вище посилки.

1. Політика забезпечення інформаційної безпеки суспільства є однією з визначальних. Основна її мета – забезпечення безпеки інформації в урядових, військових установах і відомствах, де вона має статус державної або військової таємниці, фінансово-кредитних установах, а також суб'єктах господарської діяльності, що активно працюють у сфері розроблення та реалізації стратегічно важливих інноваційних напрямів, нових технологій або займаються експортно-імпортною діяльністю. Інший напрям – забезпечення безпеки інформації на підприємствах, які активно виходять на ринок, досить стабільно функціонують та у відношенні яких можуть порушуватися різні зобов'язання щодо збереження їхніх комерційних таємниць (упровадження інновацій, нових технологій, виробничих процесів і т. д.).

2. Розвиток суспільства та глобалізація світових економічних процесів призводять до того, що поняття «відкритість суспільства» вимагає контролю супровідних його явищ – результатів і факторів підвищення інтенсивності інформаційно-комунікаційних процесів. Ці процеси, своєю чергою, характеризуються впровадженням і широким використанням інформаційних технологій. Разом із тим необхідно відзначити, що відкритість суспільства, залучення в глобальні процеси великої кількості людей, ресурсів та економік цілих країн супроводжуються також низкою негативних явищ, які безпосередньо пов'язані з використанням інформації, інформаційних продуктів і послуг.

3. Наступний аспект інформаційної безпеки визначимо як здатність суб'єкта (підприємницької структури) самому визначати рівень своєї інформаційної захищеності. Його зміст зводиться до того, що суб'єкт господарської діяльності сам формулює, регламентує та реалізує вирішення таких завдань із забезпечення інформаційної безпеки:

– визначення найбільш імовірних загроз і чинників, що впливають на них, для господарюючого суб'єкта;

– визначення найбільш уразливих місць в інформаційній системі суб'єкта;

– оцінка ризиків, пов'язаних з імовірністю виникнення та реалізації загроз;

– розроблення заходів щодо запобігання та зменшення наслідків у вигляді збитку, що наноситься у сфері інформаційної інфраструктури суб'єкта, а також інформаційних продуктів і ресурсів.

Таким чином, дослідження й аналіз існуючих підходів та концепцій до визначення інформаційної безпеки дали змогу виділити теоретичний, нормативний і прикладний напрями у сфері забезпечення інформаційної безпеки.

Методологічні аспекти організації ефективної системи безпеки підприємства й управління нею містять у собі забезпечення безпеки її ресурсів – фінансових, матеріальних, інформаційних, трудових – та безпеки їхньої взаємодії з об'єктами, що відносяться до внутрішнього та зовнішнього середовища підприємства (табл. 1).

Таблиця 1

Класифікація загроз інформаційній безпеці

Найменування загрози	Характер загрози (прояв)	Збиток
ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКА		
Відсутність нормативів і правил, що регламентують політику у сфері інформаційної безпеки	Необґрунтоване визначення рівня інформаційного захисту	Фатальний
Відсутність документації, що регламентує рівень таємності інформації, доступ до неї посадових осіб	Існуюча можливість розголошення комерційної таємниці	Сильний
Відсутність положень, посадових інструкцій відносно процедур обмеженого доступу до інформації	Неефективне управління інформаційними ресурсами	Сильний
Відсутність процедур адміністративного контролю над програмно-апаратними засобами	Неефективне управління інформаційними ресурсами	Помірний
ВИРОБНИЧО-ПРОЦЕСНА (процеси обробки й видачі інформації)		
Відсутність профілів захисту	Відсутність чітко сформульованої і зрозумілої співробітниками політики безпеки	Сильний
Несанкціонований доступ до інформації та інформаційних продуктів	Зловживання	Сильний
Відсутність процедур ідентифікації користувачів	Несанкціонований вхід в інформаційну систему	Помірний
Несанкціонована модифікація, обробка, передача інформації та інформаційних продуктів (у т. ч. з віддалених терміналів у комп'ютерних мережах)	Шахрайство. Обдурювання. Витік інформації в процесі передачі по каналах зв'язку (втрата інформацією конфіденційності, порушення доступу, втрата цілісності та модифікація авторизованої інформації)	Сильний
Відсутність процедур аутентифікації	Доступ до авторизованої інформації	Слабкий
Відсутність процедур адміністрування паролів	Порушення якісних властивостей профілів захисту	Помірний
Відсутність процедур захисту файлів	Доступ до авторизованої інформації	Слабкий
ЗАБЕЗПЕЧУВАЛЬНА		
Використання неліцензійного програмного забезпечення (системного та прикладного)	Укладання некоректних договорів	Фатальний
Несанкціоноване підключення до джерела інформації і використання інформації, що відноситься до комерційної таємниці	Доступ до винятково конфіденційної інформації (без її коректування), сканування	Сильний
Незаконна модифікація програмного забезпечення – системного та прикладного – протягом життєвого циклу інформаційної системи	Троянські коні. Логічні закладки. Програмні віруси.	Сильний
Використання «сумнівних» джерел інформації у процесах прийняття управлінських рішень	Укладення некоректних договорів із відповідними організаціями	Помірний
Відсутність регламентованих процедур тестування наявного програмного забезпечення	Відсутність чіткої організації експлуатації наявного програмного забезпечення	Сильний

Особлива увага приділяється інформаційній безпеці, яка реалізує різні схеми захисту інформації з погляду таких понять (властивостей інформації), як «цілісність», «доступність» і «конфіденційність». Використання цих понять дає змогу сформулювати безпечні режими роботи з інформацією і визначити ефективність засобів захищеності інформаційних ресурсів інформаційної системи, що експлуатується на підприємстві. При цьому дослідники застосовують відомі моделі «порушників», 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 інформаційні системи і персонал із 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 для виконання робіт, пов'язаних із модифікацією й використанням конфіденційної інформації, виявлення і протидія витоку інформації стосовно виникаючих загроз, носіями яких виступають суб'єкти.

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 поняття й визначення інформації.

Під інформацією будемо розуміти множину даних, кожна підмножина яких характеризується такими властивостями, як об'єктивність, вірогідність, адекватність, своєчасність, коректність, точність, корисність, цінність. У 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 твердження, що властивість інформації певною мірою характеризує певну функцію управління, реалізовану суб'єктом, який використовує інформацію, що призводить до такої системи тверджень.

Твердження 1. Інформація, що використовується суб'єктом відносно якої-небудь дії, повинна реалізувати (виконувати) певну функцію суб'єкта в системі (структурі) управління підприємством. Такими функціями можна розглядати функції управління, управління виробництвом, прийняття рішень, планування й т. д.

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

Твердження 2. Для ефективної реалізації своєї управлінської функції суб'єктові необхідно розвивати кількісні й якісні характеристики тієї властивості, яка є основною, обов'язковою, такою, що часто використовується (або ж групи властивостей).

Як наслідок, із нього випливає:

Твердження 3. 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.

Наведені твердження припускають використання концепції інформаційної безпеки, основні положення якої 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 і, 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 інструментальний засіб (сукупність засобів), який забезпечує безпечний розвиток властивостей інформаційних ресурсів на всіх рівнях управління підприємством.

Механізми протидії інформаційній зброї повинні базуватися на посиленні позитивних чинників – інформаційної інфраструктури і зменшенні (нейтралізації) негативних чинників, перепрограмуванні інформаційної інфраструктури на основі таких дестабілізуючих дій, як навмисна модифікація та інтерпретація інформаційних продуктів і їхніх похідних, із метою виділення таких процедур, технологій маніпулювання ними, які б дали змогу досягти переваги в матеріальній сфері.

Протидії можуть носити пасивний (нейтралізуючий) і активний характер.

Пасивні протидії можуть містити в собі вирішення таких завдань:

1. Кількісна і/або якісна оцінка поточного та необхідного рівня інформаційної безпеки за заданих рівнів конфіденційності інформації для різних рівнів управління підприємством.

2. Розроблення заходів щодо реінжинірингу системи безпеки інформаційної системи для досягнення її заданого рівня.

3. Проведення аудиту і сертифікації компонентів інформаційної системи у цілому на відповідність вимогам та існуючим стандартам інформаційної безпеки.

4. Розроблення зон відповідальності для взаємодії служб і підрозділів зі службою інформаційної безпеки підприємства. Розроблення організаційно-розпорядницької документації з координації і реалізації заходів щодо забезпечення необхідного рівня захисту з припустимими рівнями ризиків.

5. Розроблення політики і концепції забезпечення інформаційної безпеки підприємства на період 3–5 років із визначенням осіб, відповідальних за її реалізацію.

Активні протидії представляють сукупність методів, засобів, правил надання впливу на інформаційні простори (інформаційні інфраструктури) суб'єктів взаємодії з метою запобігання і нейтралізації інформаційних атак та вироблення власної політики в інформаційній сфері для забезпечення стабільного розвитку підприємства.

До основних завдань у забезпеченні активної протидії належать:

1. Збільшення «своїх» засобів і каналів інформаційного впливу на суспільну думку (захоплення, перехоплення й постановка під свій вплив різних засобів масової інформації).

2. Протидія і розроблення цільових заходів із недопущення витоку інформації.

3. Підвищення іміджу й репутації підприємства за рахунок публікації достовірної та об'єктивної інформації про підприємство в урядових, регіональних засобах масової інформації, що мають високий рівень репутації.

4. Постійна сертифікація наявного та придбаного ліцензійного устаткування, рівень інформаційної безпеки якого гарантується, що дасть змогу забезпечити імідж підприємства як такого, що має високий рівень захищеності.

5. Широке використання засобів контррозвідувальної діяльності з метою визначення місцезнаходження підслуховуючих пристроїв, засобів радіоелектронної війни, комп'ютерної хакерської діяльності.

6. Постійний контроль точок входу зовнішніх комунікаційних систем в інформаційну систему підприємства, особливо в корпоративних системах, що використовують віддалені комп'ютерні термінали, з метою виявлення спрямованого інформаційного впливу для порушення їхньої діяльності.

Формування підприємством механізмів, сполучених із механізмами прояву чинників інформаційної безпеки і безпеки ресурсів підприємства у цілому дасть змогу сформувати стійкі режими функціонування інформаційної системи і підвищити якість керованого підприємства.

Висновки з цього дослідження і перспективи подальших розвідок у даному напрямку. Інформаційні процеси є основою функціонування сучасного суспільства та «провідником», за допомогою якого реалізується взаємодія між суб'єктами ринкових відносин, власне ринку як такого та його численних структур. Їхня відкритість, досить висока розгалуженість породжують проблеми, конфлікти, пов'язані з «упровадженням» активних наступальних технологій у світовому інформаційному просторі для того, щоб одержувати переваги в матеріальній і фінансовій сферах. Інформаційна безпека визначається такими поняттями, як «інформація», «безпека», «інформаційний продукт», «інформаційна послуга», «інформаційна інфраструктура». Детермінантою інформаційної безпеки є положення про захищеність процесів зміни властивостей інформації, а також процесів, пов'язаних із різними формами її обробки. Властивості інформації, які в першу чергу визначають рівень її захищеності, визначаються суб'єктами, що провадять цю інформацію, а також виробленими ними інформаційними продуктами і послугами.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Кавун С.В. Економічна безпека підприємства: інформаційний аспект. Харків, 2014. 312 с.

2. Ковтун О.І. Стратегія підприємства : навчальний посібник. Київ, 2014. 680 с.

3. Судакова О.І., Щеглова О.Ю., Гасенко О.О. Головна характеристика механізму управління економічною безпекою розвитку підприємства. *Науковий вісник Міжнародного гуманітарного університету. Серія «Економіка і* менеджмент». 2017. № 24. С. 11–14.

4. Чумак О.В., Андрющенко І.С. Управління витратами в інформаційно-аналітичній системі підприємств ресторанного господарства : монографія. Харків, 2016. 268 с.

REFERENCES:

1. Kavun C.V. (2014) EkonomIchna bezpeka pidpriemstva [Economic security of the enterprise]. Kharkiv [in Ukrainian]

2. Kovtun O.I. (2014) Strategiya pidpriemstva [Strategy of the enterprise]. Kyiv: [in Ukrainian]

3. Sudakova O.I., Scheglova O.Yu., Gasenko O.O. (2017) Golovna harakteristika mehanizmu upravlinnya ekonomichnoyu bezpekoyu rozvitku pidpriemstva [The main characteristic of control mechanism of the economic security enterprise]. *Scientific bulletin of the International Humanitarian University. Series: "Economics and Management".* – 24. 11-14. [in Ukrainian]

4. Chumak O.V., Andrjushhenko I.S. (2016). Upravlinnja vytratamy v informacijno-analitychnij systemi pidpryjemstv restorannogo gospodarstva [Cost Management in the Information and Analytical System of Restaurant Enterprises]. Harkiv [in Ukrainian]