УДК 005.93:001.891
DOI: https://doi.org/10.36887/2415-8453-2019-4-24

Ірина Анатоліївна МАРКІНА

доктор економічних наук, професор, завідувач кафедри менеджменту, Полтавська державна аграрна академія
ORCID ID: 0000-0003-2815-4223
E-mail: iryna.markina@pdaa.edu.ua

Юрій Миколайович ГАРІЧЕВ

здобувач, Полтавська державна аграрна академія

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ТА ОРГАНІЗАЦІЙНІ ЗАХОДИ ЇЇ ЗАБЕЗПЕЧЕННЯ

Маркіна, І. А. Інформаційна безпека підприємства та організаційні заходи її забезпечення [Текст] / Ірина Анатоліївна Маркіна, Юрій Миколайович Гарічев // Український журнал прикладної економіки. – 2019. – Том 4. – № 4. – С. 209–215. – ISSN 2415-8453.

Анотація

У зв'язку із зростаючою роллю інформаційних ресурсів, а також через реальність численних загроз надзвичайно актуальні й потребують поглибленого вивчення проблеми інформаційної безпеки підприємств і організацій України. Без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку. Збільшення коштів і заходів захисту інформації, спільно з існуючими недоліками типової реалізації системи захисту інформації, збільшують навантаження на персонал підприємства й час на прийняття управлінських рішень. Водночас, менеджери підприємств сфери економіки та бізнесу відчувають певний дефіцит спеціальної літератури з питань забезпечення інформаційної безпеки як складової загальної системи економічної безпеки господарюючого суб'єкта. У зв'язку з викладеним тема дослідження представляється актуальною.

Метою дослідження є теоретичне обґрунтування організаційного забезпечення інформаційної безпеки підприємства й надання пропозицій щодо оптимізації управління нею в умовах динамічного бізнес-середовища.

В статті розглянуто наукові підходи до визначення поняття інформаційної безпеки підприємства. Авторами зазначено, що в науковій літературі відсутній єдиний погляд на сутність поняття «інформаційна безпека». Для одних це поняття відображає діяльність, стан, для інших властивість, процес, функцію, систему гарантій, здатність. Також відсутня норма, яка б містила дефініцію поняття «інформаційна безпека», враховуючи різницю між поняттями інформаційної безпеки й безпеки інформації. Авторами здійснено теоретичний поглиблений аналіз даного поняття. Поняття «інформаційна безпека» слід розглядати як стан захищеності систем обробки та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення. Виокремлено декілька напрямів досліджень змісту даного поняття. Класифіковано й уніфіковано основні заходи щодо управління інформаційною безпекою підприємств і організацій України.

Ключові слова: *загрози, захист інформації, заходи, інформаційна безпека, принципи, управління.*

© Ірина Анатоліївна Маркіна, Юрій Миколайович Гарічев, 2019

Iryna Anatoliyivna MARKINA

Doctor of economics, Professor, Head of the Department of Management,
Poltava State Agrarian Academy

Yuriy Nikolaevich GARICHEV

Applicant, Poltava State Agrarian Academy

ENTERPRISE INFORMATION SECURITY AND ORGANIZATIONAL MEASURES OF ITS

Abstract

Organization of an effective system of economic security is an important aspect of business growth in modern management conditions. Due to the large role of information resources, the reality of threats, the information security problems of enterprises and organizations in Ukraine are relevant. Without protection of the enterprise information environment, it is impossible to ensure its economic security. The heads of enterprises in the field of economics and business do not have special literature on information security. Questions of concepts, characteristics, and components of information security are not fully understood. Scientific provisions for managing information security of enterprises have not been developed.

The purpose of the study is the theoretical justification of the organizational support of the enterprise information security. The author has proposed measures to optimize information security management.

In the scientific literature there is no single view on the concept of "information security". The author carried out a theoretical analysis of this concept. The concept of "information security" is the security state of data processing and storage systems. This is to ensure the confidentiality, accessibility and integrity of information. These are measures aimed at ensuring the security of information from: unauthorized access, use, publication, destruction, alteration, viewing, verification of recordings or destruction. We have studied the research direction on the concept content of "information security". Information security management must adhere to the principles of information security. We offer the following principles: legality; planning; complexity; continuity; interaction of subjects of ensuring information security; improvement; scientific validity; technical implementation; the control; warning. The main measures for managing information security of enterprises and organizations are summarized.

Keywords: *threats, protection of information, measures, information security, principles, management.*

JEL classification: D83; M15

Вступ

В сучасних умовах динамічного бізнес-середовища одним із найважливіших аспектів забезпечення стійкого зростання бізнесу й формування позитивних результатів фінансової діяльності є організація ефективної системи економічної безпеки. Захист обумовлений здатністю органів управління підприємства на відповідних рівнях: забезпечити сталий економічний розвиток підприємства; нейтралізувати негативний вплив кризових явищ економіки; сформувати адекватну систему обліку фінансових потоків і зміцнити операційну ефективність системи контролю; забезпечити проведення робіт із захисту конфіденційності інформації, що становить комерційну таємницю тощо. У зв'язку із зростаючою роллю інформаційних ресурсів, а також через реальність численних загроз надзвичайно актуальні й потребують поглибленого вивчення проблеми інформаційної безпеки підприємств і організацій України. Без належного захисту інформаційного середовища підприємства неможливо забезпечити

його економічну безпеку. Збільшення коштів і заходів захисту інформації, спільно з існуючими недоліками типової реалізації системи захисту інформації, збільшують навантаження на персонал підприємства й час на прийняття управлінських рішень. Водночас, менеджери підприємств сфери економіки та бізнесу відчувають певний дефіцит спеціальної літератури з питань забезпечення інформаційної безпеки як складової загальної системи економічної безпеки господарюючого суб'єкта. У зв'язку з викладеним тема дослідження представляється актуальною.

Вивченням питання інформаційної безпеки займалися такі вчені, як: Абрамчук М., Богуш В, Герасименко А., Гуцу С., Деркач М., Дячков Д., Живко З., Захаркін О., Козак А., Кормич Б., Ліпкан В., Максименко Ю., Маркіна І., Марущак А., Ортинський В., Сороківська О., Петрик В. Нашинець-Наумова А., Шевченко С. та ін.

Проте залишаються дискусійними питання сутнісних і змістовних характеристик інформаційної безпеки підприємств; не визначені підходи до складових інформаційної безпеки; не розроблені наукові положення щодо управління інформаційною безпекою підприємств в сучасних умовах господарювання.

Мета дослідження

Метою дослідження є теоретичне обґрунтування організаційного забезпечення інформаційної безпеки підприємства й надання пропозицій щодо оптимізації управління нею в умовах динамічного бізнес-середовища.

Виклад основного матеріалу дослідження

Необхідно зазначити, що в науковій літературі відсутній єдиний погляд на сутність поняття «інформаційна безпека». Для одних це поняття відображає діяльність, стан; для інших – властивість, процес, функцію, систему гарантій, здатність. Також відсутня норма, яка б містила дефініцію поняття «інформаційна безпека», враховуючи різницю між поняттями інформаційної безпеки й безпеки інформації. Теоретичний поглиблений аналіз даного поняття приведено в табл. 1.

Таблиця 1. Аналіз визначень наукового поняття «інформаційна безпека»*

Автор, джерело	Визначення поняття
Баранов-ський О. І. [1]	стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення й використання, а також через негативний інформаційний вплив і негативні наслідки функціонування інформаційних технологій
Богуш В. [2]	стан захищеності інформаційного середовища, який відповідає інтересам держави й забезпечується формування, використання та можливості роз-витку незалежно від впливу внутрішніх і зовнішніх інформаційних загроз
Жарков Я. М., Бєсєдіна Л. М. [4]	стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень і захист інформаційних ресурсів країни
Калюж-ний Р. [11]	стан захищеності інформаційного простору, який забезпечує формування й розвиток цього простору в інтересах особистості, суспільства та держави
Кормич Б. [7]	стан захищеності встановлених законодавством норм і параметрів інформаційних процесів і відносин, що забезпечує необхідні умови існування держави, людини й суспільства як суб'єктів цих процесів і відносин
Ліпкан В. А., Максименко Ю. Є., Желіхов-ський В. М. [8]	стан захищеності життєво важливих інтересів особи, суспільства й держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недосто-вірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації
Ортинський В.Л., Керницький І. С., Живко З. Б. [3]	стан захищеності інформаційного простору, який забезпечує формування й розвиток цього простору в інтересах особистості, суспільства та держави

Продовження табл. 1

Автор, джерело	Визначення поняття
Мару-щак А. І. [9]	стан захищеності життєво важливих інтересів особистості, суспільства й держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність, недостовірність інформації чи негативний інформаційний вплив, через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації
Петрик В. [10]	стан захищеності особи, суспільства й держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди

**складено автором*

Поняття «інформаційна безпека» слід розглядати як стан захищеності систем обробки й зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення [6].

Нами виокремлено декілька напрямів досліджень змісту поняття «інформаційна безпека» (рис. 1).

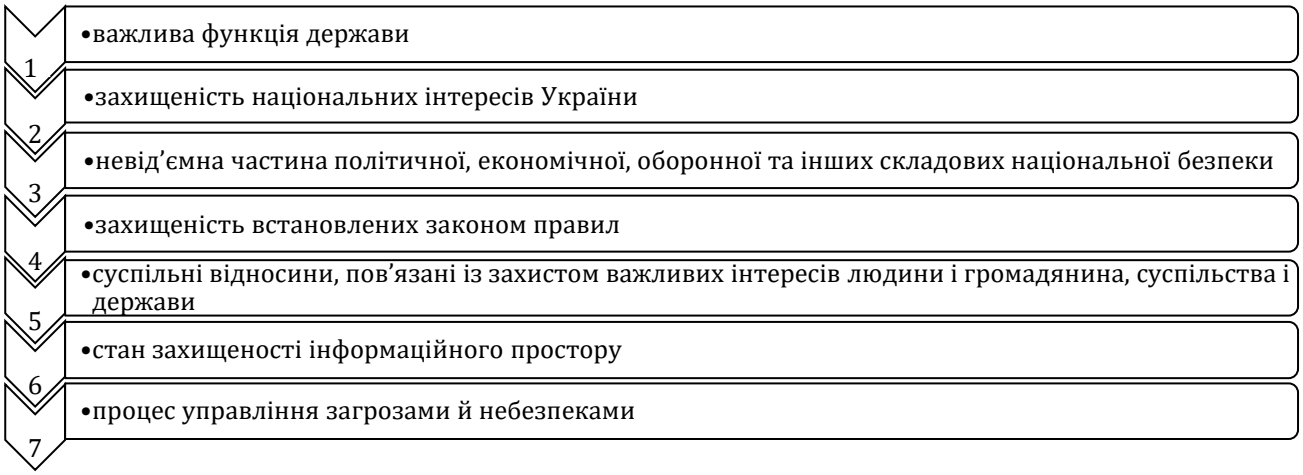

Рис. 1. Напрями досліджень змісту поняття «інформаційна безпека»

Побудова моделі управління інформаційною безпекою має дотримуватися загальноприйнятих концептуальних принципів, закладених при побудові будь-якої системи захисту інформації. Враховуючи основні тенденції в сфері забезпечення захисту інформації при управлінні інформаційною безпекою, пропонуємо підтримуватися таких концептуальних принципів:

– законність, дотримання балансу інтересів особи, суспільства й держави;
– системність;
– плановість;
– комплексність;
– безперервність;
– взаємна відповідальність суб'єктів забезпечення інформаційної безпеки, їх взаємодія;
– спадкоємність і безперервність вдосконалення;
– розумна достатність;
– персональна мінімізація повноважень;
– наукова обґрунтованість і технічна реалізація;
– обов'язковість контролю;

– превентивний характер проведення заходів інформаційної безпеки щодо заходів інших видів безпеки.

Основні заходи щодо управління інформаційною безпекою підприємств і організацій узагальнено в табл. 2.

Таблиця 2. Основні організаційні заходи забезпечення інформаційної безпеки*

Заходи	Дії
Організаційні разові заходи (проводяться одноразово і повторюються тільки при повному перегляді прийнятих рішень)	заходи щодо створення нормативно-методологічної бази захисту автоматизованих систем (розробка концепцій і інших керівних документів)
	внесення необхідних змін і доповнень в організаційно-розпорядчі документи з питань забезпечення безпеки ресурсів автоматизованих систем і дій у разі виникнення загрози (положення про підрозділи, функціональні обов'язки посадових осіб, технологічні інструкції користувачів системи і т.п.)
	створення підрозділу захисту інформації (комп'ютерної безпеки) і призначення поза-штатних відповідальних за інформаційну безпеку в підрозділах і на технологічних ділянках
	заходи щодо розробки політики безпеки, визначення порядку призначення, зміни, затвердження і надання конкретним категоріям співробітників необхідних повноважень з доступу до ресурсів системи
	розробка правил розмежування доступу до ресурсів системи
	заходи, що здійснюються при проектуванні, будівництві й обладнанні об'єктів автоматизованих систем (виключення можливості встановлення апаратури для прослуховування, виключення можливості таємного проникнення в приміщення і т.п.)
	заходи, здійснювані при розробці й введенні в експлуатацію технічних засобів і програмного забезпечення (перевірка та сертифікація використовуваних технічних і програмних засобів, документування тощо)
	визначення порядку проектування, розробки, модифікації, придбання, налагодження, прийому в експлуатацію, дослідження, зберігання й контролю цілісності програмних продуктів
	визначення порядку обліку, видачі, використання й зберігання знімних магнітних носіїв інформації, які містять еталонні та резервні копії програм і масивів інформації, архівні дані і т.п.
	визначення порядку поновлення версій використовуваних і встановлення нових системних і прикладних програм на робочих місцях захищеної системи
	проведення спецперевірок застосовуваних в автоматизованих системах засобів обчислювальної техніки й проведення заходів щодо захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень
	заходи щодо створення системи захисту автоматизованої системи й необхідної інфраструктури (організація обліку, зберігання, використання та знищення документів і носіїв із закритою інформацією, обладнання службових приміщень сейфами (шафами) для зберігання реквізитів доступу, засобами знищення паперових і магнітних носіїв конфіденційної інформації тощо)
	визначення переліку файлів і баз даних, що містять інформацію, яка становить комерційну й службову таємницю, а також вимог до рівнів їх захищеності від несанкціонованих дій при передачі, зберіганні та обробці в автоматизовану систему; виявлення найбільш ймовірних загроз для даної системи
	організація охорони й надійного пропускного режиму
	визначення переліку необхідних і таких, що регулярно проводяться, превентивних заходів і оперативних дій персоналу щодо забезпечення безперервної роботи і відновлення обчислювального процесу автоматизованих систем в критичних ситуаціях
Заходи за потребою	здійснювання кадрових змін у складі персоналу системи; заходи щодо добору й розстановки кадрів
	заходи, здійснювані при ремонті й модифікаціях обладнання та програмного забезпечення (розгляд і затвердження змін, санкціонування, перевірка вимог захисту, документальне відображення змін і т.п.)
	перевірка нового обладнання, призначеного для обробки закритої інформації, на наявність спеціально впроваджених закладних пристроїв
	оформлення юридичних документів з питань регламентації відносин з користувачами і третьою стороною про правила вирішення спорів, пов'язаних з інформаційним обміном
	обладнання систем інформатизації пристроями захисту від збоїв електроживлення й перешкод у лініях зв'язку
	оновлення технічних і програмних засобів захисту у відповідність з мінливою оперативною обстановкою

Продовження табл. 2

Заходи	Дії
Періодичні заходи, що проводяться при здійсненні або виникненні певних змін у автоматизованій системі або зовнішньому середовищі	здійснення аналізу стану й оцінки ефективності заходів і засобів захисту та вдосконалення системи захисту
	розподіл реквізитів розмежування доступу (паролів, ключів шифрування і т.п.)
	аналіз журналів реєстрації, прийняття заходів за виявленими порушеннями правил роботи
	перегляд правил розмежування доступу користувачів до ресурсів автоматизованої системи організації
Необхідні заходи, які проводяться постійно (безперервно або дискретно у випадкові моменти часу)	забезпечення достатнього рівня фізичного захисту всіх компонентів автоматизованої системи (охорона приміщень, забезпечення збереження й фізичної цілісності засобів обчислювальної техніки, носіїв інформації, протипожежна охорона, пропускний режим, і т.п.)
	заходи щодо безперервної підтримки функціонування та управління засобами захисту
	організація явного й прихованого контролю за роботою користувачів і персоналу системи
	контроль за реалізацією обраних заходів захисту в процесі проектування, розробки, введення в лад, функціонування, обслуговування й ремонту автоматизованих систем
	постійний (силами служби безпеки) й періодичний (із залученням сторонніх фахівців) аналіз стану й ефективності заходів і засобів захисту

* *систематизовано автором*

Висновки та перспективи подальших розвідок

Отже, організаційні заходи захисту інформації складають сукупність заходів щодо підбору, перевірки й навчання персоналу, який бере участь у всіх стадіях інформаційного процесу [5].

В умовах динамічного бізнес-середовища інформаційна безпека є невід'ємною складовою системи економічної безпеки підприємства. Відповідно, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку.

Надійне забезпечення інформаційної безпеки – неодмінна умова переходу на модель стійкого розвитку не тільки окремого суб'єкта господарювання, а й національної економіки в цілому.

Список літератури

1. Барановський О. І. Фінансова безпека. К. : Фенікс, 1999. 338 с.
2. Богуш В., Юдін О. Інформаційна безпека держави. К. : «МК-Прес», 2005. 432 с.
3. Економічна безпека підприємств, організацій та установ: навчальний посібник / Ортинський В. Л., Керницький І. С., Живко З. Б. та ін. К. : Правова єдність, 2009. 544 с.
4. Жарков Я. М., Бєсєдіна Л. М. Напрямки зовнішнього інформаційно-психологічного впливу на Україну. *Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка*. 2009. № 19. С. 15-19.
5. Захаркін О. О., Абрамчук М. Ю., Деркач М. А. Інформаційні системи та технології у фінансових установах. Суми : Вид-во СумДУ, 2007. 80 с. URL: http://elkniga.info/book_188.html.
6. Інформаційна безпека. Економічний енциклопедичний словник. URL: http://zalik.org.ua/index.php?newsid=25011

7. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. … докт. юрид. наук : спец. 12.00.07. М-во освіти і науки України, Нац. ун-т внутр. справ. Харків. ХНУВС, 2004. 42 с.
8. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К. : КНТ, 2006. 280 с. URL: http://pidruchniki.com/component/option,com_jdownloads/Itemid,999999/catpid,349/task,view.annotation
9. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 92-95.
10. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Юридичний журнал. 2009. № 5. С. 122-134.
11. Питання концепції реформування інформаційного законодавства України / Калюжний Р., Говловський В., Цимбалюк В., Гузалюк М. К.: НТУУ «КПІ», Міністерсово освіти і науки України, 2000. С. 17-21.

References

1. Baranovskyi, O. I. (1999). *Finansova bezpeka.* [Financial security]. Feniks. Kyiv. Ukraine.
2. Bohush, V. and Yudin, O. (2005). *Informatsiina bezpeka derzhavy.* [Information security]. «MK-Pres». Kyiv. Ukraine.
3. *Ekonomichna bezpeka pidpryiemstv, orhanizatsii ta ustanov.* (2009). [Economic security of enterprises, organizations and institutions]. Ortynskyi, V. L., Kernytskyi, I. S., Zhyvko, Z. B. ta in. K. : Pravova yednist. Kyiv. Ukraine.
4. Zharkov, Ya. M. and Biesiedina, L. M. (2009). «Directions of external information and psychological influence on Ukraine». *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu im. T. Shevchenka*. no. 19, pp. 15-19.
5. Zaharkin, O. O., Abramchuk, M. Ju. and Derkach, M. A. (2007). Informacijni sistemi ta tehnologii u finansovih ustanovah [Information systems and technologies in financial institutions]. Sumy. Ukraine. Available at: http://elkniga.info/book_188.html
6. Informational security. Economic encyclopedic dictionary. Available at: http://zalik.org.ua/index.php?newsid=25011
7. Kormich, B. A. (2004). *Orhanizatsiino-pravovi osnovy polityky informatsiinoi bezpeky Ukrainy*. [Organizational and legal bases of information security policy Ukraine]. Abstract LL.D. Thesis. 12.00.07. Kharkiv. Ukraine.
8. Lipkan, V. A. Maksymenko, Yu. Ye. and Zhelikhovskyi, V. M. (2006). *Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii.* [Information security Ukraine in terms of European integration. KNT. Kyiv. Ukraine. Available at: http://pidruchniki.com/component/option,com_jdownloads/Itemid,999999/catpid,349/task,view.annotation
9. Marushchak, A. I. (2011). «Information and legal directions of information security problems research». *Derzhavna bezpeka Ukrainy*. no. 21. pp. 92-95.
10. Petryk, V. (2009). «The essence of information security of the state, society and person». *Yurydychnyi zhurnal*. no. 5. pp. 122-134.
11. *Pytannia kontseptsii reformuvannia informatsiinoho zakonodavstva Ukrainy.* (2000). [The question of reform concepts of information legislation Ukraine]. Kaliuzhnyi, R., Hovlovskyi, V., Tsymbaliuk, V. and Huzaliuk, M. *Zbirnyk «Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini»*. NTUU «KPI». Ministersovo osvity i nauky Ukrainy. SBU. Kyiv. Ukraine.

Стаття надійшла до редакції 08.09.2019 р.