6. Shelest, V.V. (2009), "Management of Financial Security of Trust Society", *Actual problems of the economy*, no. 3, pp. 181-184.

7. Hotomlyanskiy, O.L. and Znahurenko, P.A. (2007), "A comprehensive assessment of the financial condition of the enterprise", *Finance of Ukraine*, no. 1, pp. 111-117.

8. Burkovska, A.V. and Solovyov, O.Yu. (2012), "A comprehensive approach to assessing the financial situation of the company", *Collected works of Poltava State Agrarian Academy*, Iss. 1(4), vol. 2, pp. 73-77.

9. Galushka, V.V. and Antonenko, V.N. (2009), "Justification of the recommended values of analytic financial performance of enterprises", *Collected works of Donetsk National Technical University, Series: Economic*, Iss. 36-2, pp. 204-209.

10. Evdokimov, F.I., Mizina, O.V. and Borodina, O.O. (2002), "Summative evaluation of the financial and economic security of the enterprise", *Collected works of Donetsk National Technical University, Series: Economic*, Iss. 46, pp. 6-12.

11. Poberezhniy, S.M., Plastun, O.L. and Bolgar, T.M. (2010), *Finansova bezpeka bankivskoyi diyalnosti: navchalniy posibnik dlya samostiynogo vivchennya distsiplini "Bezpeka bankiv"* [Financial security of banking activities: a manual for self-study course "Security of banks"], DVNZ "UABC NBU", Sumy, Ukraine.

УДК 005.93:005.8:001.891

ІНФОРМАЦІЙНА БЕЗПЕКА ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Северина С.В., к.е.н., асистент

Запорізький національний університет
Україна, 69600, м. Запоріжжя, вул. Жуковського, 66

sev.s@inbox.ru

Підприємствам різних галузей доводиться функціонувати в умовах високої складності, невизначеності і динамічності навколишнього середовища. За рахунок інформатизації світового ринку суб'єкти господарювання мають доступ до будь-якої інформації, що створює конкуренцію у виробничій сфері. У зв'язку з цим виникає нагальна потреба у створенні не тільки єдиного інформаційного простору, але й адекватного механізму організації інформаційної безпеки на підприємствах. Ця діяльність набуває особливої актуальності на сучасному етапі, коли поширюються різноманітні способи ворожого конкурентного впливу. Не менш важливим є забезпечення інформаційної безпеки на рівні країни. Ця проблема потребує нагального вирішення, особливо в контексті тривалої інформаційної агресії з боку Російської Федерації. Події останніх місяців довели, що Україна зовсім не готова протидіяти атакам в інформаційній сфері. Наслідком цієї бездіяльності стали численні людські жертви, анексія Криму та окупація Донецької та Луганської областей. У статті визначено сутність та основні складові інформаційної безпеки підприємства, а також приведено нагальні проблеми інформаційної політики менеджменту на підприємстві. Наведено законодавчі акти, які регулюють процес впровадження та забезпечення системи захисту інформації в Україні. Розглянуто поняття, призначення інформаційної безпеки і методів вдосконалення інформаційного середовища діяльності підприємства на сучасному етапі розвитку економічної науки. Класифіковано та уніфіковано найбільш уживані методи для забезпечення інформаційної безпеки. Для забезпечення конфіденційності інформації надано рекомендацій щодо підвищення рівня інформаційної безпеки вітчизняних підприємств.

Ключові слова: інформаційна безпека підприємства, потенційні загрози, служба інформаційної безпеки, способи захисту, засоби захисту.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Северина С.В., к.э.н., ассистент

Запорожский национальный университет
Украина, 69600, г. Запорожье, ул. Жуковского, 66

Предприятиям различных отраслей приходится работать в условиях высокой сложности, неопределенности и динамичности окружающей среды. За счет информатизации мирового рынка субъекты хозяйствования имеют доступ к любой информации, что создает конкуренцию в производственной сфере. В связи с этим возникает насущная необходимость в создании не только единого информационного пространства, но и адекватного

механизма организации информационной безопасности на предприятиях. Эта деятельность приобретает особую актуальность на современном этапе, когда получают распространение различные способы враждебного конкурентного влияния. Не менее важным является обеспечение информационной безопасности на уровне страны. Эта проблема требует неотложного урегулирования, особенно в контексте длительной информационной агрессии со стороны Российской Федерации. События последних месяцев показали, что Украина совсем не готова противодействовать атакам в информационной сфере. Следствием этого бездействия стали многочисленные человеческие жертвы, аннексия Крыма и оккупация Донецкой и Луганской областей. В статье определена сущность и основные составляющие информационной безопасности предприятия, а также приведены насущные проблемы информационной политики менеджмента. Приведены законодательные акты, регулирующие процесс внедрения и обеспечения системы защиты информации в Украине. Рассмотрены понятие, назначение информационной безопасности и методов совершенствования информационной среды деятельности предприятия на современном этапе развития экономической науки. Классифицированы и унифицированы наиболее употребляемые методы для обеспечения информационной безопасности. В целях обеспечения конфиденциальности информации было предоставлено рекомендаций по повышению уровня информационной безопасности отечественных предприятий.
Ключевые слова: информационная безопасность предприятия, потенциальные угрозы, служба информационной безопасности, способы защиты, средства защиты.

INFORMATION SECURITY AND METHODS FOR ITS PROTECTION

Severina S.V., Ph.D. Economics, assistant

Zaporizhzhya National University
Ukraine, 69600, Zaporizhzhya, Zhukovsky str., 66

Different industries have to operate under conditions of high complexity, uncertainty and dynamic environment. Due to the informatization of the world market entities have access to any information that competes in the industrial sphere. In this regard, there is an urgent need not only to create a common information space, but also adequate mechanism for organizing information security in enterprises. This activity is of particular relevance at the present stage, when are spreading various ways hostile competitive effects. No less important is information security at the country level. This problem requires urgent departure, especially in the context of sustained information aggression by the Russian Federation. The events of recent months have shown that Ukraine is not ready to counter attacks in the information sphere. The result of this omission led to numerous casualties, the occupation and annexation of the Crimea, Donetsk and Lugansk regions. In the article the essence and main elements of information security, and given the urgent problem of information management policies in the enterprise. Indicated legislation governing implementation and ensuring information security system in Ukraine. Determined concept, purpose and methods of information security improvements of enterprise information environment at the present stage of development economics. Classification and unification of the most commonly used methods for information security. In order to ensure the confidentiality of information were provided recommendations for improving the information security of domestic enterprises.
Key words: information security company, potential threats, information security service, method sofprotection, protection.

ПОСТАНОВКА ПРОБЛЕМИ

У сучасному суспільстві інформація стала одним із найважливіших стратегічних ресурсів, що забезпечує подальший розвиток підприємства. Саме тому інформація, як і решта ресурсів, потребує особливого захисту.

Проблема інформаційної безпеки набула особливого значення в сучасних умовах широкого застосування автоматизованих інформаційних систем.

У зв’язку із зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, а також через реальність численних загроз проблема інформаційної безпеки вимагає до себе постійної і значної уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставин, які мають до того ж різну фізичну природу, що переслідують різні цілі і викликають різні наслідки, приводять до необхідності комплексного підходу при вирішенні цієї проблеми.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Загалом інформація пронизує всі сфери життя суспільства, створюючи нову основу розвитку економіки, культури і взагалі нову характеристику соціуму. Вивченням питання інформаційної безпеки займалися такі вчені, як С. Ф. Гуцу, Б. А. Кормич, А. І. Марущак, О. А. Сороківська [1-4].

Класичними чинниками економічної безпеки країни, за визначенням О. А. Кулініч, є «активізація попиту і відповідна за обсягами та структурою реакція пропозиції» [5, с. 59-60]. Учений під класичними чинниками економічної безпеки розуміє чинники сталого економічного зростання, які досліджує через вивчення та порівняння зростання внутрішнього попиту, зміни його структури за секторами та верствами населення.

Живко З. Б. та Керницькою М. І. проаналізовано чинники позитивного та негативного, прямого та опосередкованого впливу у різних сферах безпеки, зазначено роль індикаторів і чинників економічної безпеки, визначено та досліджено суть соціально-економічної безпеки [6, с. 14-15].

Кавун С. В. визначає життєвий цикл економічної безпеки підприємства та досліджує основні рівні економічної безпеки підприємства [7, с. 17-18]. Однак у комплексі чинники інформаційної безпеки підприємства, їхній вплив на конкурентоспроможність бізнесу, забезпечення безпеки персоналу та розвиток самої системи безпеки фірми ще достатньо не досліджені.

Проте проблема інформаційної безпеки підприємства залишається недостатньо дослідженою. Це пов'язано з тим, що автори значну увагу приділяють забезпеченню інформаційної безпеки держави, а також з відсутністю цілеспрямованого підходу до проблеми в цілому у тих учених, які розглядали роль інформації в діяльності підприємства.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета статті полягає у вивченні основних вимог щодо забезпечення інформаційної безпеки підприємства, в розробці основних заходів щодо попередження виникнення загроз втрати та знищення інформації.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Усі економічно розвинуті країни світу використовують переваги інформаційних технологій у виробничій, комерційній та банківських сферах. Це пояснюється тим, що традиційні методи не дозволяють зорієнтуватись в сучасному інформаційному потоці і проаналізувати динамічні процеси економічної діяльності підприємства. Швидше за все розвиваються технології, по'вязані з глобальною комп'ютерною мережею Інтернет, що призвело до появи таких нових категорій, як електронна торгівля, електронний бізнес, електронний уряд та ін. [3, с. 32].

Зі зростанням науково-технічного прогресу зростає і необхідність вирішення проблеми інформаційної безпеки. Інформація – це чинник, який може призвести до технологічних аварій, військових та політичних конфліктів, дезорганізації державного управління, фінансової системи.

Необхідно зазначити, що в науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека підприємства», що є надзвичайно актуальним на сучасному етапі розвитку інформаційних технологій і супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору.

Так, Б. Кормич трактує інформаційну безпеку як стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин [2, с. 15].

Деякі вчені розглядають інформаційну безпеку як стан захищеності життєво важливих інтересів особистості, суспільства і 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 [3, с. 72]. Інформаційну безпеку суспільства також визначають як неможливість заподіяння шкоди його духовній сфері,

культурним цінностям, соціальним регуляторам поведінки людей, інформаційній інфраструктурі й повідомленням, що передаються за її допомогою [8, с. 64].

Із розвитком інформатизації, яка спостерігається останніми роками, з'явилась ще одна глобальна проблема – інформаційна безпека. Більша частина інтересів підприємства визначається станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні дії з боку зовнішніх або внутрішніх джерел можуть задавати шкоду цим інтересам і становлять реальну загрозу для подальшої діяльності підприємства.

Не викликає сумніву і той факт, що між рівнем економічної безпеки і інформаційною складовою існує пряма залежність. Як показує практика, будь-яка акція, спрямована проти господарюючого суб'єкта, розпочинається зі збору інформації, саме тому питання інформаційної безпеки давно ввійшли до головних пріоритетів практично всіх великих підприємств. Усе більше керівників розуміють, наскільки небезпечною може бути інсайдерська інформація, системи обробки інформації і дії співробітників, які беруть участь у діяльності підприємства [9].

Для регулювання економічної безпеки на підприємстві створюється служба інформаційної безпеки, що має виявляти і наочно демонструвати власникам підприємства весь спектр загроз в інформаційній сфері. Завдання керівників служби переконати, що протистояти загрозам можна тільки на основі створення і упровадження ефективних систем захисту інформації [2].

Виділимо найпоширеніші види потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій:

– відсутність регламентованого доступу до файлів даних;

– вільне втручання в програмне забезпечення;

– відсутність протоколювання змін у програмному забезпеченні;

– відсутність регламентації користувачів інформації;

– відсутність дублювання важливих документів на документальних носіях даних;

– часті удосконалення одного і того ж програмного забезпечення різними особами;

– відсутність схем інформаційного забезпечення рівнів управління;

– наявність непідзвітних посадових осіб у системі управління тощо [8, 10-12].

Створюючи системи захисту на підприємстві, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні. По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту. Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки підприємства дозволив сформулювати основні функції та завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки. У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями [9]:

1) розробка методології та методик аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення;

2) організація і здійснення конкретних видів діяльності із захисту інформації;

3) експлуатація технічних засобів захисту інформації;

4) аудит і контроль функціонування системи інформаційної безпеки підприємства [13, с. 131].

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист від зовнішніх і від внутрішніх загроз [14, с. 106].

Технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті. Сьогодні використовується шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання.

Усі перераховані методи націлені на побудову ефективної технології захисту інформації, при якій виключено витрати через недбалість і успішно відображено різні види загроз. Під перешкодою розуміється спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

Маскування – способи захисту інформації, що передбачає перетворення даних у форму, не придатну для сприйняття сторонніми особами. Для розшифровки потрібне знання принципу.

Управління – способи захисту інформації, при яких здійснюється управління над всіма компонентами інформаційної системи.

Регламентація – найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

Примус – методи захисту інформації, тісно пов’язані з регламентацією, що припускають введення комплексу заходів, при яких працівники змушені виконувати встановлені правила. Коли використовуються способи впливу на працівників, за яких вони виконують інструкції з етичних і особистісним міркувань, то йдеться про спонукання [15].

Способи захисту інформації передбачають використання певного набору засобів. Для запобігання втрати та витоку таємних даних використовуються засоби:

– фізичні;
– апаратні;
– програмні;
– апаратно-програмні;
– законодавчі;
– криптографічні та організаційні методи.

Фізичні засоби захисту – це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об’єктів. Вони реалізуються на базі ЕОМ, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до компонентів інформаційних систем, що захищаються.

Апаратні засоби захисту – це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв’язку тощо.

Програмні засоби захисту, які вмонтовані до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

Апаратно-програмні засоби захисту – це засоби, які основані на синтезі програмних та апаратних засобів.

Законодавчі засоби – комплекс нормативно-правових актів, що регулюють діяльність людей, які мають доступ до відомостей, що охороняються, і визначають міру відповідальності за втрату або крадіжку секретної інформації.

Організаційні заходи захисту інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу [16].

ВИСНОВКИ

Отже, у сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. Своєю чергою, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити ефективну систему управління інформаційною безпекою. Сутність викладеного дає підстави стверджувати, що в сучасних умовах, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку.

ЛІТЕРАТУРА

1. Гуцу С. Ф. Правові основи інформаційної діяльності : навч. посіб. / С. Ф. Гуцу. — Х. : Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. — 48 с.
2. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Б. А. Кормич ; Нац. ун-т внутр. справ. — Х., 2004. — 42 с.
3. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А. І. Марущак // Державна безпека України. — 2011. — № 21. — С. 92—95.
4. Сороківська О. А. Інформаційна безпека підприємства : нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету. — 2010. — № 2, т. 2. — С. 32—35.
5. Кулініч О. А. Структурні чинники економічної безпеки України / О. А. Кулініч // Шлях України до економічної безпеки : матеріали наук.-практ. конф. — Х. : ХНУВС, 2007. — С. 59—63.
6. Живко З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. І. Керницька. — Львів : Ліга-Прес, 2008. — 345 с.
7. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия / С. В. Кавун // Управління розвитком. — Х. : ХНЕУ, 2008. — Вип. 6. — С. 17—21.
8. Smieliauskas W. Auditing: An International Approach / W. Smieliauskas, K. Bewley. — McGraw-Hill Ryerson Higher Education, 2006. — 800 p.
9. Иванов О. В. Информационная составляющая современных войн / О. В. Иванов // Вестн. Моск. ун-та: сер. 18 : Социология и политология. — 2004. — № 4. — С. 64—70.
10. Гришина Н. В. Организация комплексной системы защиты информации / Н. В. Гришина. — М. : Гелиос АРВ. — 2007. — 256 с.
11. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубєв, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. Р. А. Калюжного. — Запоріжжя : Просвіта, 2001. — 252 с.
12. Porter B. Principles of External Auditing / B. Porter, D. Hatherly, Jon Simon. — [3rd edition]. — Wiley, 2008. — 816 p.
13. Марунич А. В. Захист інформації як основна складова економічної безпеки підприємства / А. В. Марунич // Управління розвитком. — 2014. — № 14. — С. 130—132.
14. Гордієнко С. Б. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії / С. Б. Гордієнко, О. С. Микитенко, В. Г. Данильчук // Вісник ДУІКТ. — 2013. — № 1. — С. 104—107.
15. Ясенев В. Н. Информационная безопасность в экономических системах : учеб. пособ. [Электронный ресурс] / В. Н. Ясенев. — Н. Новгород : Изд-во ННГУ, 2006. — Режим доступа : http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html.
16. Захаркін О. О. Інформаційні системи та технології у фінансових установах : конспект лекцій [Електронний ресурс] / О. О. Захаркін, М. Ю. Абрамчук, М. А. Деркач. — Суми : Вид-во СумДУ, 2007. — 80 с. — Режим доступу : http://elkniga.info/book_188.html.

REFERENCES

1. Gucu, S.F. (2009), *Pravovi osnovi informacijnoi diialnosti* [Legal basis of the information], tutorial, Nac. aerokosm. un-t "Hark. aviac. in-t", Kharkiv, Ukraine.
2. Kormich, B.A. (2004), "Organizational and legal bases of information security policy Ukraine", 12.00.07, Thesis abstract LL.D., Kharkiv, Ukraine.
3. Marushhak, A.I. (2011), "Information and research areas of the legal problems of information security", *Derzhavna bezpeka Ukraini*, no. 21, pp. 92-95.
4. Sorokivska, O.A. and Gevko, V.L. (2010), "Enterprise Information Security: New Threats and Prospects", *Visnik Hmelnickogo nacionalnogo universitetu*, no. 2, Vol. 2, pp. 32-35.
5. Kulinich, O.A. (2007), "Structural factors of economic security of Ukraine", *Shliah Ukraini do ekonomichnoi bezpeky: materiali naukovo-praktichnoi konferencii* [Ukraine's path to economic security. Proceedings of the Conference], Kharkov, HNUVS, pp. 59-63.
6. Zhivko, Z.B. and Kernicka, M.I. (2008), *Socialno-ekonomichna bezpeka* [Socio-economic security], Liga-Pres, Lviv, Ukraine.
7. Kavun, S.V. (2008), "Economic security of the system life cycle", *Upravlinnja rozvitkom*, vol. 6, pp. 17-21.
8. Smieliauskas, W. and Bewley, K. (2006), "Auditing: An International Approach", McGraw-Hill Ryerson Higher Education, New York, USE.
9. Ivanov, O.V. (2004), "Information component of modern warfare", *Vestn. Mosk. un-ta*, *Ser. 18: sociology and political science*, no. 4, pp. 64-70.
10. Grishina, N.V. (2007), *Organizaciia kompleksnoy sistemy zashhity informacii* [Organization Integrated system of information protection], Gelios ARV, Moscow, Russia.
11. Golubev, V.O., Havlovskyi, V.D. and Tsymbaliuk, V.S. (2001), *Informacijna bezpeka: problemi borotbi zi zlochinami u sferi vikoristannja kompjuternih tehnologij* [Information security: challenges to combat crimes in the sphere of computer technologies], zag. red. Kaljuzhnij, R.A., Prosvita, Zaporozhye, Ukraine.
12. Porter, B., Hatherly, D. and Simon, Jon (2008), "Principles of External Auditing", 3rd edition, Wiley.
13. Marunich, A.V. (2014), "Information security as a basic component of economic security", *Upravlinnja rozvitkom*, no. 14, pp. 130-132.
14. Gordiєnko, S.B., Mikitenko, O.S. and Danilchuk, V.G. (2013), "Methods and Recommendations Information security consulting company"», *Visnik DUIKT*, no. 1, pp. 104-107.
15. Jaseniv, V.N. (2006), *Informacijna bezpeka v ekonomichnih sistemah* [Information security in economic systems], tutorial, NNDU, Novgorod, Russia, available at: http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html (access March 1, 2016).
16. 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], lecture notes, Sumy, Ukraine, available at: http://elkniga.info/book_188.html (access March 1, 2016).

УДК 65.012.8:336:658.1(477)

ОСНОВНІ ПРИНЦИПИ ТА МІСЦЕ ФІНАНСОВОЇ БЕЗПЕКИ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Худолєй Л.В., аспірант

Запорізький національний університет
Україна, 69600, м. Запоріжжя, вул. Жуковського, 66

lina_kozobash@ukr.net

Питання фінансової безпеки є актуальним для сучасних підприємств, зважаючи на те, що на переважній більшості підприємств оцінюванням фінансової безпеки практично не займаються, а це вимагає практичних і теоретичних досліджень у цій сфері. Однією з найважливіших проблем ефективного розвитку підприємства в ринкових умовах господарювання є забезпечення фінансової безпеки як основної складової економічної безпеки підприємства. Головна мета фінансової безпеки підприємства полягає в гарантуванні його стабільного