

3. Скороход І.П. Напрямки та механізм реалізації державної інноваційно-інвестиційної політики регіону / І.П. Скороход, Н.А. Завгородня // Глобальні та національні проблеми економіки. – 2015. – Випуск №4. – С.261–264.

4. EEA Report No 30/2016. Environmental indicator report 2016 – In support to the monitoring of the 7th Environment Action Programme. [Electronic resource]. – Access mode : <http://www.eea.europa.eu/publications/environmental-indicator-report-2016-2014>. – The name of the screen

5. Innovation in Food and Agriculture. OECD. [Electronic resource]. – Access mode : <http://www.oecd.org/tad/agricultural-policies/innovation-food-agriculture.htm>. – The name of the screen

6. Innovations at Work in Agriculture. USDA [Electronic resource]. – Access mode : <https://newfarmers.usda.gov/innovations-work-agriculture>. – The name of the screen

7. Regulation (EU) No 1305/2013 of 17 December 2013 on support for rural development by the European Agricultural Fund for Rural Development (EAFRD) [Electronic resource]. – Access mode : <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013R1305>. – The name of the screen

8. Rural development 2014–2020. Agriculture and rural development. European Commission [Electronic resource]. – Access mode : https://ec.europa.eu/agriculture/rural-development-2014-2020_en. – The name of the screen

I.O. ТАРАСЕНКО,

д.е.н., професор, Київський національний університет технологій та дизайну

Н.В. ЦИМБАЛЕНКО,

к.е.н., доцент, Київський національний університет технологій та дизайну

О.М. БАТЕЧКО,

студент, Київський національний університет технологій та дизайну

Формування системи інформаційної безпеки

У статті досліджено теоретичні підходи до визначення інформаційної безпеки підприємства. Проаналізовано методичні підходи та розроблено практичні рекомендації щодо ефективної системи інформаційної безпеки підприємницької діяльності.

Ключові слова: економіка, ресурси, динаміка, безпека, діяльність, організація, інформація.

И.А. ТАРАСЕНКО,

д.э.н., профессор, Киевский национальный университет технологий и дизайна.

Н.В. ЦИМБАЛЕНКО,

к.э.н., доцент, Киевский национальный университет технологий и дизайна.

А.Н. БАТЕЧКО,

студент, Киевский национальный университет технологий и дизайна

Формирование системы информационной безопасности

В статье исследованы теоретические подходы к определению информационной безопасности предприятия. Проанализированы методические подходы и разработаны практические рекомендации по эффективной системе информационной безопасности предпринимательской деятельности.

Ключевые слова: экономика, ресурсы, динамика, безопасность, деятельность, организация, информация.

I. TARASENKO,

Doctor of Economics, professor of Kyiv National University of Technology and Design.

N. TSYMBALENKO,

candidate of economic sciences associate professor of Kyiv National University of Technology and Design.

O. BATECHKO,

student Kyiv National University of Technology and Design

Formation of information security

In the article the theoretical approaches to the definition of information security. Analyzed the methodological approaches and practical recommendations for effective information security system of entrepreneurial activity.

Keywords: economy, resources, dynamics, safety, activity, organization, information.

Постановка проблеми. Аналіз сучасного стану розвитку інформаційних систем є особливо актуальним питанням, адже успішне функціонування організації у значній мірі залежить від вдалого керівництва, яке базується на обґрунтуванні перспективних концепцій розвитку згідно з своєчасною, достовірною та

повною інформацією, яку може поставляти відповідна інформаційна система.

Аналіз останніх досліджень і публікацій. Визначення поняття та сутності системи управління інформаційною безпекою підприємства висвітлюють у працях такі вчені: І.М. Вядрової, В.М. Гейця, А.А. Гри-

ценка, О.В. Дзюблюка, Б.Л. Луціва, І.О. Лютого, В.І. Міщенко, А.М. Мороза, О.А. Пересади, М.І. Савлука, В.М. Федосова, А.В. Шаповалова та інших [1–10].

Невирішені частини дослідження. У процесі своєї діяльності будь-яка компанія оперує інформацією як специфічним товаром значної вартості. Володіння достовірною і своєчасною інформацією, а також її оптимальне використання забезпечує ефективне функціонування суб'єкта господарювання як цілісного комплексу. Тому проблема забезпечення інформаційної безпеки будь-якої компанії є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій, яка супроводжується постійними інформаційними загрозами – як зовнішніми, так і внутрішніми. Саме тому, забезпечення інформаційної безпеки підприємства є невід'ємною частиною його фінансово-економічної безпеки.

Мета статті. Визначити особливості методичного забезпечення організації системи інформаційної безпеки підприємства, які висвітлені в наукових працях зарубіжних та вітчизняних вчених.

Виклад основного матеріалу. Система інформаційної безпеки підприємства – це комплекс організаційно-управлінських, технічних, профілактичних заходів, спрямованих на захист інтересів підприємства від зовнішніх та внутрішніх загроз [4].

Інформаційна безпека підприємства на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку.

Управління інформаційної безпекою підприємства являє собою систему принципів і методів розробки та реалізації управлінських рішень, пов'язаних із забезпеченням захисту його пріоритетних інформаційних та фінансових інтересів від зовнішніх та внутрішніх загроз [5, с. 12].

Забезпечення інформаційної безпеки в загальній постановці проблеми може бути досягнуте лише при

взаємопов'язаному розв'язку трьох складових, що представлені на рис. 1.

Тому, відокремимо найбільш гострі проблеми розвитку теорії й практики інформаційної безпеки:

1) створення теоретичних основ і формування науково-методологічного базису управління інформацією в контексті забезпечення економічної безпеки підприємства, що дозволяють адекватно описувати процеси в умовах значної невизначеності й непередбачуваності прояву дестабілізуючих факторів (інформаційних загроз);

2) розробка науково-обґрунтованих нормативно-методичних документів з питань забезпечення інформаційної безпеки на базі дослідження й класифікації загроз інформації й вироблення стандартних вимог до захисту;

3) стандартизація підходів до створення систем захисту інформації й раціоналізація схем і структур управління захистом на об'єктовому, регіональному й державному рівнях.

Відповідно до викладеного загальна схема забезпечення інформаційної безпеки може бути представлена так, як показано на рис. 2.

З наведеного випливає, що, по-перше, розвиток теорії інформаційної безпеки обумовлюється основними напрямками розвитку теорії захисту інформації як першої складової загальної проблеми інформаційної безпеки; по-друге, розвиток теорії інформаційної безпеки визначається рівнем вивчення і розробки другої складової інформаційної безпеки – захисту від інформації.

Модель управління системою забезпечення інформаційної безпеки підприємства надана на рис. 3.

Головне завдання системи управління полягає у ефективному використанні всіх власних ресурсів підприємства та можливостей зовнішніх суб'єктів інформаційної безпеки для організації комплексної протидії небезпекам, загрозам та ризикам. Ефективність системи інформаційної безпеки багато в чому залежить від рівня взаємодії і координації діяльнос-

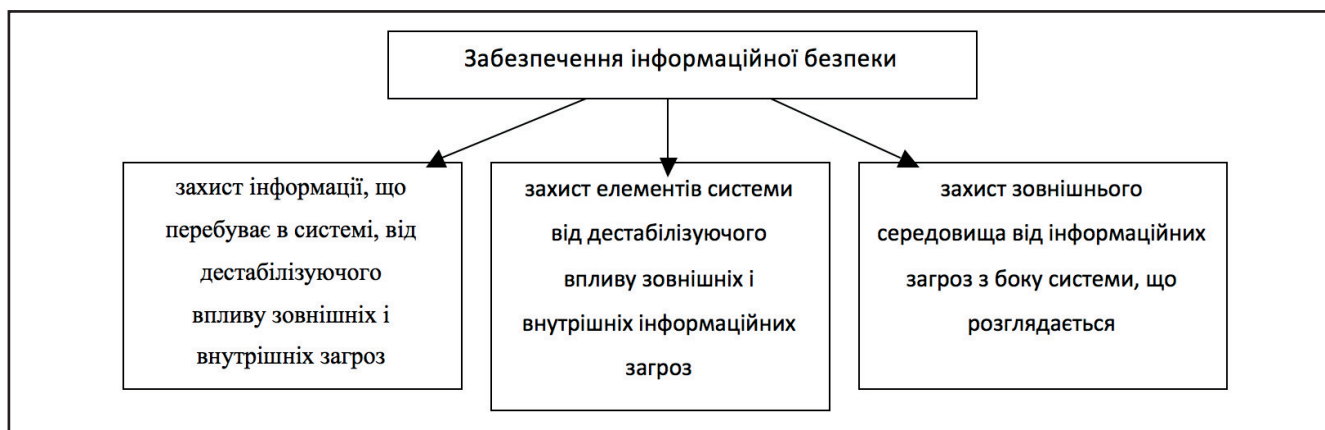


Рисунок 1. Складові забезпечення інформаційної безпеки [1]

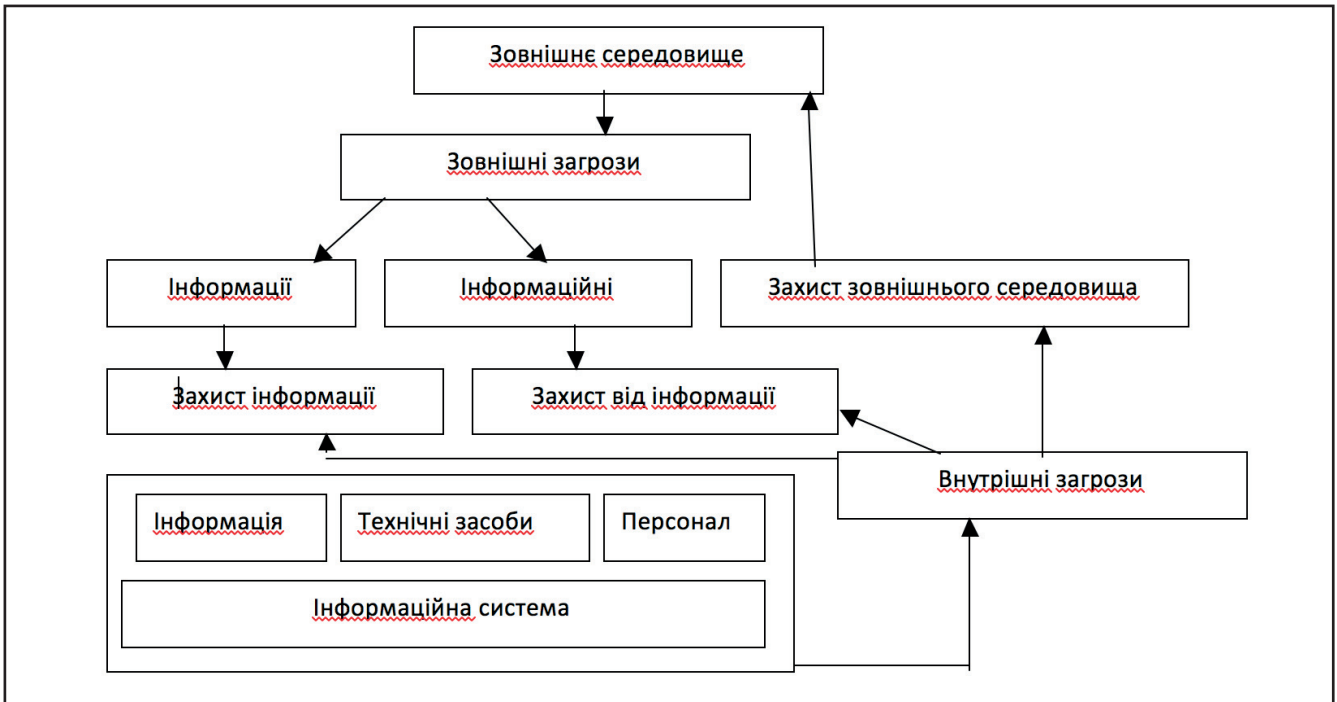


Рисунок 2. Загальна схема забезпечення інформаційної безпеки [4, с. 158]



Рисунок 3. Модель управління системою забезпечення інформаційної безпеки підприємства (побудовано автором)

ті всіх суб'єктів системи забезпечення інформаційної безпеки підприємства по протидії всіх небезпек, погроз і ризиків. Взаємодія в системі інформаційної безпеки підприємства — це узгоджені дії всіх сил і засобів за завданнями, напрямками та часом заради

досягнення конкретної мети з протидії несприятливих факторів у зовнішній і внутрішньому середовищі підприємства.

Організаційні заходи щодо створення і забезпечення функціонування комплексної системи захисту на

ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗЕЙ ТА ВИДІВ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ

підприємствах є тією основою, яка об'єднує різні заходи захисту в єдину систему.

Оцінка рівня інформаційної складової економічної безпеки здійснюється на основі аналізу показників використання інформаційних ресурсів підприємства: продуктивності інформації, інформаційної озброєності, захищеності інформаційних ресурсів.

Розглянемо модель системи інформаційної безпеки підприємства ТОВ «Пеймастер», побудовану відповідно до стандарту (ISO 15408 «Загальні критерії оцінки безпеки інформаційних технологій») і даних аналізу ризиків (ISO 17799 «Стандарт побудови ефективної системи безпеки»). Ця модель відповідає спеціальним нормативним документам із гарантування інформаційної безпеки, прийнятих в Україні, міжнародному стандарту ISO/IEC 15408 «Інформаційна технологія – методи захисту, критерії оцінки інформаційної безпеки», стандарту ISO/IEC 17799 «Управління інформаційною безпекою» і враховує тенденції розвитку вітчизняної нормативної бази з питань інформаційної безпеки. Деталізований опис загальної мети побудови системи безпеки об'єкта виражається сукупністю чинників або критеріїв, які уточнюють мету. Сукупність чинників є основою визначення вимог до системи (вибір альтернатив).

Модель системи інформаційної безпеки підприємства ТОВ «Пеймастер» – це сукупність зовнішніх і внутрішніх чинників, їх вплив на стан інформаційної безпеки підприємства ТОВ «Пеймастер» і забезпечення ресурсів. На рис. 4. наведена модель системи інформаційної безпеки підприємства.

В моделі системи інформаційної безпеки підприємства ТОВ «Пеймастер» представлені напрямки впливу між наступними факторами:

– загрозами інформаційній безпеці, які характеризуються ймовірністю виникнення та реалізації;

– вразливістю системи інформаційної безпеки, що впливає на ймовірність реалізації загрози;

– ризиками, що відображають передбачуваний збиток в результаті реалізації загрози інформаційній безпеці.

В даному випадку інформаційна безпека ідентифікується як стан інформації, інформаційних ресурсів та інформаційних систем при якому забезпечується захист інформації (даних) від витоку, крадіжки, втрат, несанкціонованого знищення, викривлення, модифікації (підробки), копіювання, блокування бази даних тощо. Тому захист інформації повинен включати комплекс правових, організаційних і технічних засобів та заходів, спрямованих на запобігання неправомірних дій з інформацією. Метою діяльності підприємства в сфері ІБ повинно бути забезпечення збалансованого і успішного виконання своїх функцій, досягнення сталого ведення бізнесу в умовах ризиків, що можуть привести до порушення конфіденційності, цілісності, доступності інформації, а також до порушення стійкості функціонування її мереж зв'язку та інформаційних систем.

Таким чином, деякі показники ТОВ «Пеймастер» мають позитивні тенденції та перебувають у рамках нормативних значень, але інші мають відверто негативні значення та тенденції розвитку, через те не можна однозначно стверджувати, що підприємство має стійке довгострокове фінансове становище та не буде мати проблем у перспективі, якщо керівництво не відреагує на відхилення від нормативів показників і не застосує превентивних заходів щодо покращення стану підприємства та недопущення настання кризи у майбутньому.

ТОВ має досить стабільне становище, в якому спостерігається тенденція до покращення своїх показників. В результаті аналітичних розрахунків видно, що інтегральна оцінка фінансового стану ТОВ «Пеймастер» за 2015 рік склала 70 балів, що відповідає II класу і дозволяє оцінити фінансовий стан компанії

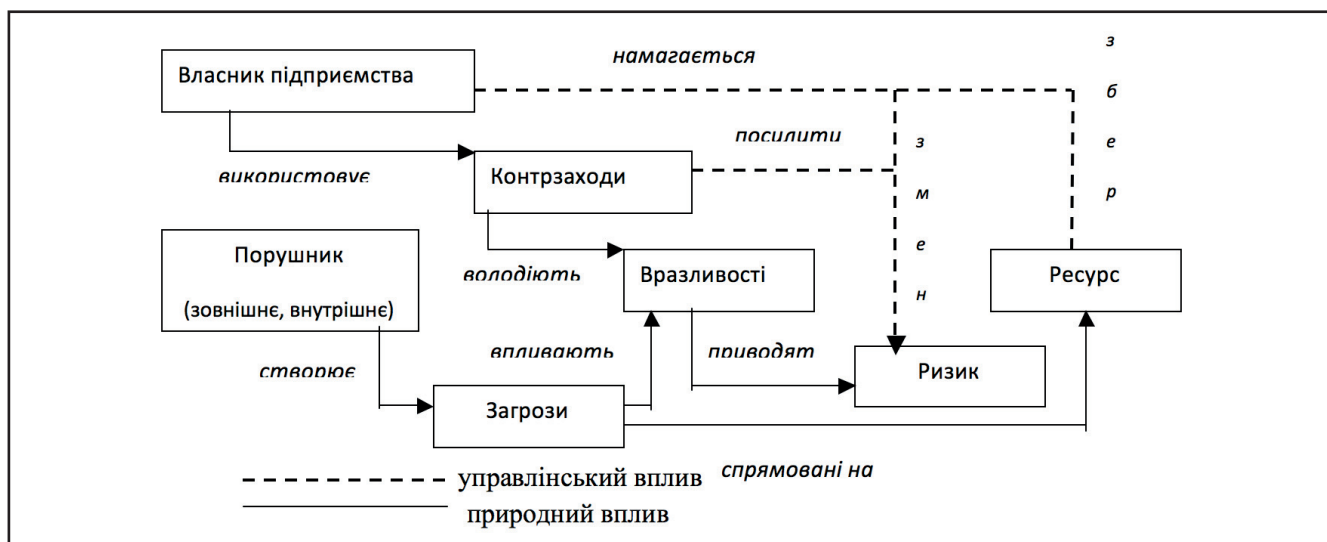


Рисунок 4. Система безпеки підприємства ТОВ «Пеймастер» в інформаційній сфері

вище нормального, що свідчить про високий рівень показників ліквідності, платоспроможності і фінансової стійкості. Кожного року рівень інформаційної безпеки ТОВ «Пеймастер» підвищується, що спричинено заходами по захисту інформації керівництвом товариства. Інформаційна безпека забезпечується створенням на підприємстві ефективної структури управління інформаційною безпекою. При цьому необхідно досягти погодженого застосування різноманітних та уніфікованих методів і механізмів забезпечення інформаційної безпеки в межах усіх процесів та інформаційних активів.

Для ефективної системи інформаційної безпеки підприємницької діяльності безумовно необхідно, щоб на ТОВ «Пеймастер» існував оновлений інформаційно-аналітичний підрозділ, що є складовою служби безпеки, функціями якого є захист будь-якої інформації організації, висвітлення обстановки всередині і поза межами підприємства, вчасно одержувати випереджальну інформацію про життєво важливі для підприємства процеси і знаходити засоби її оптимального використання.

Висновки

Для ефективної системи інформаційної безпеки підприємницької діяльності безумовно необхідно, щоб на ТОВ «Пеймастер» існував оновлений інформаційно-аналітичний підрозділ, що є складовою служби безпеки, функціями якого є захист будь-якої інформації організації, висвітлення обстановки всередині і поза межами підприємства, вчасно одержувати випереджальну інформацію про життєво важливі для підприємства процеси і знаходити засоби її оптимального використання. Метою аудиту фінансової безпеки ТОВ «Пеймастер» є правильність і своєчасність визначення загроз фінансовій безпеці, існуючих ризиків здійснення фінансової діяльності, чинників, що призвели до певного стану фінансової безпеки, можливостей підприємства щодо утримання фінансової безпеки на належному рівні, а також розроблення заходів щодо забезпечення фінансової безпеки ТОВ «Пеймастер».

Список використаних джерел

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій / Г.Я. Аніловська. [Електронний ресурс]. – Доступний з http://nbuv.gov.ua/portal/chem_biol/nvnliti/18_9/270_Anilowska_18_9.pdf
2. Баланда А.Л. Інформаційно-аналітичне забезпечення економічної безпеки суб'єктів підприємницької діяльності: стан та перспективи розвитку // Управління проектами та розвиток виробництва. – 2011. – № 1 (37). – С. 3–8.
3. Богуш В. М. Інформаційна безпека держави / Богуш В. М., Юдін О. К. – К.: «МК-Прес», 2009. – 432 с.
4. Домарев В. В. Безопасность информационных технологий. Системный подход: – К.: ООО «ТИД «ДС», 2004. – 992 с.
5. Захаренко К. Категорія «інформаційної безпеки» у вітчизняному науковому дискурсі [Електронний ресурс] / К. Захаренко // Гуманітарний вісник державного вищого навчального закладу «Переяслав-Хмельницький державний педагогічний університет ім. Г. С. Сковороди». Філософія. – 2015. – Вип. 37. – С. 106–117. – Режим доступу: http://nbuv.gov.ua/UJRN/gvphrph_2015_37_15
6. Игнатьев, В. А. Информационная безопасность современного коммерческого предприятия [Текст] : монография / В. А. Игнатьев. – Старый Оскол : ООО «ТНТ», 2005. – 448 с.
7. Танцюра М.Ю. Проблемні аспекти визначення інформаційного аудиту / М.Ю. Танцюра // Молодая наука Крыма – 2007: материалы науч. конф. (Симферополь, 19 октября 2007 г.) / Национальная академия природоохранного и курортного строительства. – Симферополь, 2007. – С. 165–166.
8. Танцюра М.Ю. Система управління інформаційною безпекою підприємства / М.Ю. Танцюра // Развитие инновационной культуры общества: проблемы и перспективы: материалы науч.-практ. конф. (Симферополь, 2007 г.) / Крымский институт бизнеса. – Симферополь: «Азгол-Пресс», 2007. – С. 159–161.
9. Чуруброва С. М. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень [Електронний ресурс] / С. М. Чуруброва // Проблеми програмування. – 2016. – № 4. – С. 97–103.
10. Щербина, В. М. Інформаційне забезпечення економічної безпеки підприємств та установ / В. М. Щербина // Актуальні проблеми економіки. – 2006. – № 10. – С. 220–225.