DOI: https://doi.org/10.32782/2524-0072/2022-43-49

УДК 651.012.7

# МЕТОДИ УПРАВЛІННЯ КОРПОРАТИВНОЮ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

# METHODS OF MANAGEMENT OF CORPORATE INFORMATION SECURITY

**Чубаєвський Віталій Іванович**
кандидат політичних наук, доцент,
Державний торговельно-економічний університет;
директор директорату стратегічного планування та європейської інтеграції
Міністерства внутрішніх справ
ORCID: https://orcid.org/0000-0001-8078-2652

**Chubaievskyi Vitalii**
State University of Trade and Economics

У статті застосовано методи та прийоми теоретичного узагальнення, порівняльного аналізу та синтезу для дослідження обґрунтування системи методів управління інформаційною безпекою підприємства. Здійснено узагальнення наукових підходів до формування механізму економічної безпеки підприємства. Створено наукове підґрунтя для розробки механізму формування корпоративної інформаційної безпеки, елементами якого є об'єкти, суб'єкти, мета, функції та методи. Визначено, що підприємство самостійно обирає методи управління інформаційною безпекою залежно від особливостей внутрішнього і зовнішнього середовища. Доведено, що застосування системи методів управління інформаційною безпекою гарантує реалізацію економічних інтересів підприємства. Обгрунтовано, що організаційно-правові методи включають в себе моделювання процесів захисту корпоративної інформації, комплаєнс та розробку регламентних документів.

**Ключові слова:** управління, корпоративна інформаційна безпека, підприємство, економічні методи, організаційно-правові методи, технічні методи.

The article applies the methods and techniques of theoretical generalization, comparative analysis and synthesis using the study of the justification of the system of methods of managing information security of the enterprise. A generalization of scientific approaches to the formation of the mechanism of economic security of the enterprise was carried out. A scientific basis has been created for the development of a mechanism for the formation of corporate information security, the elements of which are objects, subjects, goals, functions and methods. It was determined that the company independently chooses information security management methods depending on the characteristics of the internal and external environment. It has been proven that the application of the system of information security management methods ensures the realization of the economic interests of the enterprise. It is substantiated that the organizational and legal ones include the methodology of modeling the processes of corporate information protection, compliance and the development of regulatory documents. The elements of the mechanism of formation of corporate information security are considered and the objects, subjects, goals, tasks, functions and methods of influence are defined. Economic methods of managing corporate information security and methods of modeling the enterprise's business processes are presented. A description of corporate information security modeling methods and automated information risk management methods is offered. The generalization of scientific approaches to the formation of the mechanism of economic security of the enterprise, the elements of which are objects, subjects, purpose, functions and methods, provided research and substantiation of the system of methods of managing the information security of the enterprise, taking into account the peculiarities of the internal and external environment and the selected protection strategy. Economic, organizational, legal and technical methods of information security management are proposed for use, the application of which will ensure the realization of the economic interests of the enterprise by protecting corporate information, solving the tasks of ensuring the integrity, confidentiality and availability of information for the implementation of the functions of the mechanism of formation of corporate information security.

**Keywords:** management, corporate information security, enterprise, economic methods, organizational and legal methods, technical methods.



© Чубаєвський В.І.

**Постановка проблеми.** Нагальна актуальність та необхідність ефективного захисту корпоративної інформації в умовах воєнного стану потребує запровадження дієвих механізмів та організації процесу такого захисту в межах підприємства. Відтак власники та топ-менеджери мають володіти певним баченням формування корпоративної інформаційної безпеки.

Зважаючи на те, що корпоративна інформаційна безпека спрямована на забезпечення стійких фінансових результатів та стійкого розвитку підприємства, нарощення його вартості (тобто підпорядкована основній меті та завданням його економічної діяльності), механізм її формування грунтується на теорії економічних механізмів та інтегрується в механізм управління підприємством, відповідно включаючи не лише економічні важелі, але і економічні методи. Широке застосування спеціалізованих інформаційних технологій, потребує включення до складу такого механізму низки технічних методів.

**Аналіз останніх досліджень і публікацій.** Проблеми управління корпоративною інформаційною відображені у працях вітчизняних та закордонних учених: Ж. Козінського, М. Верес, П. Перерви [1; 2; 3], С. Нагі, М. Сікорської [3], Т. Кобєлєва [4], С. Богомолова [5], М. Мельник [6], В. Степанова [7], Д. Дячкова [8], Т. Савельева, О. Панаско, О. Пригодюк [9].

Наявні дослідження сприяють розвитку теорії та методології управління корпоративною інформаційною безпекою. Водночас євроінтеграційні процеси в Україні, воєнний стан та необхідність виходу вітчизняних підприємств з кризового стану потребують розробки механізму формування економічної безпеки підприємства. Відтак розв'язання зазначених питань сприятиме підвищенню ефективності управління економічною безпекою. Це свідчить про важливість та практичну значущість окреслених проблем та обґрунтовує актуальність їх вирішення. Проте нині бракує досліджень, що стосуються вивчення можливостей застосування суб'єктами господарювання аналітичних інструментів управління корпоративною інформацією для уникнення загроз і забезпечення ефективного функціонування.

**Метою статті** є дослідження та обґрунтування системи методів управління інформаційною безпекою підприємства залежно від особливостей внутрішнього і зовнішнього середовища, обраної стратегії захисту.

Теоретичним та методологічним підґрунтям дослідження є праці вітчизняних та закордонних вчених з питань управління інформаційною безпекою підприємства. Методи теоретичного узагальнення використано для характеристики механізму економічної безпеки, порівняльного аналізу та синтезу – для обґрунтування застосування інструментів та методів управління інформаційною безпекою господарювання, що обумовлює трансформацію інформаційних систем та гарантує їх безпеку.

**Виклад основного матеріалу дослідження.** Критичний аналіз, узагальнення та розвиток сучасних наукових підходів до формування механізму економічної безпеки підприємства та її інформаційної складової зокрема, створили підгрунтя механізму формування корпоративної інформаційної безпеки, елементами якого є об'єкти, суб'єкти, мета, завдання, функції, методи (табл. 1).

Перелік методів впливу на стан інформаційної безпеки з одного боку є далеко невичерпним, а з іншого – достатньо варіативним. Підприємство обирає методи управління інформаційною безпекою залежно від особливостей внутрішнього і зовнішнього середовища, обраної стратегії засхисту тощо (табл. 2).

Організаційно-правові методи включають в себе моделювання бізнес-процесів, в тому числі процесів захисту корпоративної інформації, комплаєнс та розробку регламентних документів.

Для моделювання бізнес-процесів в сучасній практиці використовується декілька різних методів, в основі яких лежить як структурний, так і об'єктно-орієнтований підходи до моделювання.

Серед найбільш поширених методів моделювання бізнес-процесів можна виокремити: метод функціонального моделювання SADT (IDEF0); метод моделювання процесів IDEF3; моделювання потоків даних DFD; метод ARIS; метод Ericsson-Penker; метод технології Rational Unified Process (табл. 3).

Моделювання бізнес-процесів є основою для їх оптимізації, оцінювання вартості, вдосконалення бізнес-моделі, в тому числі в частині формування корпоративної інформаційної безпеки.

Наступним елементом організаційно-правових методів є комплаєнс – відносно нове поняття в діловому середовищі України. Запровадження комплаєнсу є ініціативою підприємства. Його наявність завжди засвідчує високу корпоративну культуру, прозоріцсть та інноваційність в системі запровадження інструментів та технологій управління [1; 2; 4; 5; 17; 18; 19; 20].

Загалом комплаєнсом є частина системи управління / контролю в організації, пов'язана

Таблиця 1

**Елементи механізму формування корпоративної інформаційної безпеки**

| Елементи | Коротка характеристика |
|---|---|
| Об'єкти | Структурні елементи корпоративного інформаційного простору: інформаційне поле; віртуальна реальність; інформаційний процес; інформаційна культура; технічні засоби; технологічні засоби; регламенти та норми |
| Суб'єкти | Служба безпеки, IT-служба, юридична служба, топ-менеджери, відповідальні за процеси та центри фінансової відповідальності, окремі особи, що мають доступ до конфеденційної інформації |
| Мета | Забезпечення реалізації економічних інтересів підприємства шляхом захисту корпоративної інформації |
| Завдання | Забезпечення цілісності, конфеденційності та доступності інформації |
| Функції | Ідентифікація загроз інформаційній безпеці; формування організаційної структури служби безпеки; оцінювання та аналіз загроз інформаційній безпеці; розробка стратегії захисту та планів захисту корпоративної інформації; координація роботи служби безпеки з іншими службами підприємста. |
| Методи впливу | *Економічні*: аналіз бізнес-процесів; система збалансованих показників; стратегічні карти; карта ризиків; методи інтегрального аналізу; прикладний інформаційний аналіз; споживчий індекс; додана економічна вартість; вихідна економічна вартість; управління портфелем активів; оцінка дійсних можливостей; метод життєвого циклу штучних систем; сукупна вартість володіння; функціонально-вартісний аналіз; метод експертних оцінок. |
| | *Організаційно-правові:* моделювання бізнес-процесів; комплаенс; формування регламентів та положень |
| | *Технічні: – методи моделювання інормаційної безпеки:* Модель Bell-LaPadula (BLP), Модель Biba, Модель Clark-Wilson (CW), Дискреційна (матрична) модель, Модель Адепт-50, Модель MITER ATT & CK TM", "Модель алмазу". *– автоматизовані системи управління інформаційними ризиками:* CRAMM, CORAS,OCTAVE, Risk Watch, Oracle Crystal Ball |

*Джерело: розроблено автором*

з ризиками невідповідності, недотримання вимог законодавства, нормативних документів, правил і стандартів наглядових органів, галузевих асоціацій та саморегулюючих організацій, кодексів поведінки. Такі ризики невідповідності в кінцевому підсумку можуть виявлятися у формі застосування юридичних санкцій або санкцій регулюючих органів, фінансових або репутаційних (іміджевих) втрат як результат невідповідності законам, загальноприйнятим правилам і стандартам [3].

В системі корпоративної інформаційної безпеки комплаєнс орієнтується саме на уникнення ризиків умисного витоку конфіденційної інформації від персоналу підприємства, неумисного витоку інформації шляхом порушення встановлених внутрішніх стандартів та регламентів зберігання і передавання інформації, порушення національного законодавства в сфері інформації, що може призводити до іміджевих та фінансових втрат. В банківській сфері, де запровадження комплаєнсу регламентується відповідним законодавством, виокремлюють два принципові підходи до його організації: «Rule based approach», заснований на дотриманні норми і передбачає мінімальний рівень організації комплаєнс в банку – виконується тільки те, що імперативно вимагає закон; «Risk based approach», заснований на аналізі ризиків.

Саме такий підхід рекомендується іноземним банкам як національними регуляторами, так і міжнародними структурами (Вольфсбергська група, Базельський комітет банків і банківського нагляду), є домінуючим в Європі. В Україні він також рекомендований для впровадження центральним банком, однак в українській банківській практиці є менш поширеним, ніж підхід, заснований на нормі.

Якщо розглядати комплаєнс як інструмент формування корпоративної інформаційної безпеки, його доцільно запроваджувати у формі «Risk based approach», який узгоджується з іншими інструментами формування корпоративної інформаційної безпеки.

Таблиця 2

**Економічні методи управління корпоративною інформаційною безпекою**

| Назва | Ідентифікація загроз | Аналіз | Планування |
|---|---|---|---|
| Прикладний інформаційний аналіз (*Applied Information Economics, AIE*) | + | + | + |
| Споживчий індекс (*Customer Index, CI*) | – | + | – |
| Додана економічна вартість (*Economic Value Added, EVA*) | – | + | – |
| Вихідна економічна вартість (*Economic Value Sourced, EVS*) | + | + | + |
| Управління портфелем активів (*Portfolio Management, PM*) | + | + | + |
| Оцінка дійсних можливостей (*Real Option Valuation, ROV*) | + | + | + |
| Метод життєвого циклу штучних систем (*System Life Cycle Analysis, SLCA*) | + | + | + |
| Система збалансованих показників (*Balanced Scorecard, BSC*) | - | + | + |
| Сукупна вартість володіння (*Total Cost of Ownership, TCO*) | - | + | – |
| Функціонально-вартісний аналіз (*Activity Based Costing, ABC*) | - | + | + |
| Метод експертних оцінок | + | + | + |
| Метод дисконтованого грошового потоку (*DCF*) | +- | + | - |
| Метод індексу дохідності (*PI)* | - | + | - |
| Метод чистої приведеної вартості (*NPV*) | +- | + | - |
| Метод імітаційного моделювання | + | + | + |
| Метод генетичних алгоритмів | + | + | + |
| Аналіз бізнес-процесів | + | + | - |
| Стратегічні карти | - | - | + |
| Карта ризиків | + | + | - |
| Методи інтегрального аналізу | +- | + | - |
| Сценарний підхід | + | - | + |
| Метод нечітких множин | + | - | + |
| Метод Ісікави | + | + | - |

*Джерело: розроблено автором*

Третьою групою методів формування інформаційної безпеки є технічні, в межах яких варто виокремити методи моделювання корпоративної безпеки та автоматизовані системи управління інформаційними ризиками (табл. 4, табл. 5).

Компанія при формуванні політики управління корпоративною інформаційною безпекою може обирати за основу певний з варіантів описаних підходів, розробляти власний підхід, комбінувати елементи окремих технологій тощо.

**Висновки.** Узагальнення наукових підходів до формування механізму економічної безпеки підприємства**,** елементами якого є об’єкти, суб’єкти, мета, функції та методи, забезпечило дослідження та обґрунтування системи методів управління інформаційною безпекою підприємства з урахуванням особливостей внутрішнього і зовнішнього середовища та обраної стратегії захисту. Запропоновано до використання економічні, організаційно-правові та технічні методи управління інформаційною безпекою, застосування яких забезпечить реалізацію економічних інтересів підприємства шляхом захисту корпоративної інформації, вирішення завдань забезпечення цілісності, конфіденційності та доступності інформації для реалізації функцій механізму формування корпоративної інформаційної безпеки.

Таблиця 3

**Методи моделювання бізнес-процесів підприємства**

| Методи | Коротка характеристика |
|---|---|
| SADT (Structured Analysis and Design Technique) | Вважається класичним методом підходу до управління на основі процесів, базовим принципом якого є структуризація діяльності організації у відповідності з її бізнес-процесами; використовується для моделювання штучних систем середньої складності |
| IDEF3 | Частина сімейства стандартів IDEF; використовується для моделювання послідовності виконання дій і їх взаємозалежностей в рамках процесу. Метод отримав визнання серед системних аналітиків як доповнення до методу функціонального моделювання IDEF0. |
| DFD (Data Flow Diagrams) | Ієрархія функціональних процесів, що пов'язані потоками даних. Мета такого представлення полягає у демонстрації того, як кожен процес перетворює свої вхідні дані у вихідні і виявлення зв'язків між цими процесами. |
| ARIS (Architecture of Integrated Information System) | Комплекс засобів аналізу і моделювання діяльності підприємства. Його методичну основу складає сукупність різноманітних методів моделювання, що відображають різні погляди на системи. ARIS підтримує чотири типи моделей, які віддзеркалюють різні аспекти системи, що досліджується. |
| Ericsson-Penker | Автори методу Ericsson-Penker створили свій профіль UML для моделювання бізнес-процесів – Ericsson-Penker Business Extensions, ввівши набір стереотипів, які описують основні категорії бізнес-моделі: процеси, ресурси, правила і цілі діяльності підприємства. |
| Rational Unified Process | Метод спрямовано насамперед на створення основи для формування вимог до ПЗ. Передбачає побудову двох базових моделей: моделі бізнес-процесів (Business Use Case Model); моделі бізнес-аналізу (Business Analysis Model), яка являє собою розширення моделі варіантів використання (Use Case) UML шляхом введення набору стереотипів – Business Actor (стереотип діючої особи) та Business Use Case (стереотип варіанту використання). |

*Джерело: систематизовано автором за [11; 12; 13; 14; 15; 16]*

Таблиця 4

**Характеристика методів моделювання корпоративної інформаційної безпеки**

| Методи | Коротка характеристика |
|---|---|
| Модель Bell-LaPadula (BLP) | Базується на політиці конфіденційності і визначає поняття захищеного стану; повністю математично формалізована. |
| Модель Biba | Інтегрована модель; наявність рівнів інтеграції та додаткової властивості – виклику, що відповідає за можливість суб'єкта надсилати сервісні запити. |
| Модель Clark-Wilson (CW) | В повній мірі забезпечує безпеку та підзвітність переходів у системі за рахунок вибору необхідного для такої ситуації режиму роботи з даними. |
| Дискреційна (матрична) модель | Має більш практичне спрямування, оскільки стан системи захисту можна описати тріадою (на основі термінів матричної моделі). |
| Модель Адепт-50 | Модель безпеки, яка розглядає 4 групи об'єктів безпеки: користувачі, завдання, термінали та файли. |
| Модель MITER ATT & CK TM" | База знань про тактики та методи формування інформаційної політики, базовані на реальних спостереженнях; використовується як основа для розробки конкретних моделей та методологій загроз, для приватного сектора користувачів та уряду. |
| "Модель алмазу" ("Diamond Model") | Визначає політику інформаційної безпеки об'єкта на основі аналізу чотирьох ознак: зловмисника, інформаційної інфраструктури, можливостей та об'єкта впливу. |
| " Піраміда болю" ("The Pyramid of Pain") | Вибір політики інформаційної безпеки грунтується на градуюванні загроз від слабких до критичних |
| Модель "глибинного захисту" | Передбачає розшарування механізмів інформаційної безпеки і тим самим підвищує безпеку системи в цілому. |

*Джерело: систематизовано автором за [6; 7; 8; 9; 20]*

Таблиця 5

**Характеристика автоматизованих методів управління інформаційними ризиками**

| Методи | Коротка характеристика | Переваги | Недоліки |
|---|---|---|---|
| CRAMM | Британський метод, що має відомий підхід до кількісного і якісного розрахунку ІР. Його основними цілями є: автоматизація управління ризиками, оптимізація фінансових витрат на управління, оптимізація часу на супровід систем безпеки компанії, підтримка безперервності бізнесу | Використовує комплексний підхід до оцінювання ризиків державних і комерційних організацій, застосовує техно логії оцінювання загроз і за непрямими факторами з можливістю верифікації результатів, має широку базу знань по контрзаходах і володіє універсальністю і адаптованістю під профілі різних організацій. | Вимагає спеціальної підготовки і високої кваліфікації аудитора, процес є досить трудомістким і може обраховуватись місяцями безперервної роботи аудитора, не дозволяє створювати власні шаблони звітів або модифікувати існуючі; припускає використання лише методів зниження рівня ризиків ІБ. |
| CORAS | Інструмент, що дозволяє документувати, створювати звіти про результати аналізу шляхом моделювання ризику. У цій методології інформаційні системи представлені як складний комплекс з урахуванням людського фактора, а не тільки на основі використовуваних технологій. | Програмний продукт, що реалізує цю методологію, є безкоштовним і не потребує значних ресурсів для установки; методика проста у використанні і не вимагає спеціальних знань. | Не передбачена періодичність проведення оцінювання ризиків і оновлення їх величин; не дозволяє оцінити ефективність інвестицій, вкладених у впровадження заходів безпеки. |
| Risk Watch | Сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів. | Як критерії для оцінювання та управління ризиками використовуються «очікувані річні втрати» та оцінка «повернення інвестицій»; орієнтована на точне кількісне оцінювання співвідношення втрат від загроз безпеці і затрат на створення системи захисту. | Отримані оцінки ризиків (математичне очікування втрат) далеко не вичерпують розуміння ризику з системних позицій – метод не враховує комплексний підхід до інформаційної безпеки |
| OCTAVE | Метод оперативного оцінювання критичних загроз, активів і вразливостей і вказує на те, що персонал несе відповідальність за встановлення стратегії безпеки організації. | Простота у використанні і наочність вихідних даних; швидке впровадження і використання в організаціях і установах різного профілю; регулярне проведення оцінювання ризиків та оновлення їх величин як частини процесу оцінювання ризиків. | Не використовується такий спосіб управління ризиками, як обхід (виключення); не дає кількісного оцінювання ризиків інформаційній безпеці, проте якісне оцінювання може бути використане у визначенні кількісної шкали їх ранжування. |
| Oracle Crystal Ball | Додаток до Microsoft Excel для моделювання бізнес-процесів, визначення ризиків, прогнозування невизначених даних і оптимізації результатів. | Простота у використанні і наочність вихідних даних | |

*Джерело: систематизовано автором за [10; 20]*

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Kocziszky, György Anti-corruption compliance in the enterprise's program. *Стратегічні перспективи розвитку економічних суб'єктів в нестабільному економічному середовищі : зб, тез наук, робіт 2-ї Всеукр, наук.-практ. інтернет-конф. з міжнар. участю, 28-30 листопада 2017 р.* 2017. С. 164–167.

2. Kocziszky, György Compliance risk in the enterprise / G.Kocziszky, M.Veres Somosi, T.O.Kobielieva. *Стратегії інноваційного розвитку економіки України: проблеми, перспективи, ефективність "Форвард–2017" : тр. 8-ї Міжнар, наук.-практ. Internet-конф. студ. та молодих вчених, 27 грудня 2017 р.* Харків : НТУ ХПІ, 2017. С. 54–57.

3. Nagy Szabolcs Current evaluation of the patent with regarding the index of its questionnaire. *Сучасні підходи до креативного управління економічними процесами : матеріали 9-ї Всеукр наук-практ, конф. 19 квітня 2018 р.* Київ : НАУ, 2018. С. 21–22.

4. Кобєлєва Т. О. Сутність та визначення комплаєнс-ризику. *Вісник Національного технічного університету ХПІ. Економічні науки.* 2020. № 1 (3). С. 116–121.

5. Мельник М.О. Аналіз побудови моделі політики інформаційної безпеки підприємства. *Системи обробки інформації.* 2017. Вип. 2(148). С. 126–128.

6. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики. *Державне будівництво.* 2016. № 2. URL: http://www.kbuapa.kharkov.ua/e-book/db/2016- 2/doc/1/02.pdf.

7. Дячков Д. В. Формування моделі політики інформаційної безпеки на основі концепції “глибинного захисту”. *Підприємництво і торгівля*. 2019. № 25. С. 116–121.

8. Савельева Т. В., Панаско О. М., Пригодюк О. М. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2018. № 1. С. 81–88.

9. Бабенко Л. Основи програмної інженерії : навчальний посібник. Київ : Знання, 2001. 269 с.

10. Гундарь К. Захист інформації в комп’ютерних системах: навчальний посібник. Київ : Корнейчук, 2000. 152 с.

11. Цегелик Г. Чисельні методи. Львів : Вид. центр ЛНУ ім. Івана Франка, 2004. 408 с.

12. Kocziszky, György Reputational compliance. *Дослідження та оптимізація економічних процесів "Оптимум–2017" : тр. 13-ї Міжнар.наук.-практ, конф. 6-8 грудня 2017 р.* Харків : НТУ "ХПІ", 2017. С. 140–143.

13. Sikorska M. Compliance service at guest services enterprises. *Менеджмент розвитку соціально-економічних систем у новій економіці : матеріали Міжнар, наук.-практ, інтернет-конф. 19 жовтня 2017 р.* Полтава: ПУЕТ, 2017. С. 389–391.

14. Климко Т. Ю. Корпоративний комплаєнс як превентивний захід боротьби з шахрайством. *Економіка і Фінанси.* 2015. № 6–7. С. 25.

15. Козирева Н. А. Внутрішній контроль і комплаєнс. *Внутрішній контроль в кредитній організації.* 2015. № 1. С. 65.

16. Чуруброва С.М. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень. *Проблеми програмування.* 2016. № 4. С. 97–103.

17. Замула А. А., Северинов А. В., Корнієнко М. А. Аналіз моделей оцінки ризмків інформаційної безпеки для побудови системи захисту інформації. *Наука і техніка Повітряних Сил Збройних Сил України.* 2014. № 2 (15). С. 133–138.

18. Гарасим Ю. Р., Ромака В. А., Рибій М. М. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. *Вісник Національного університету "Львівська політехніка". Сер. Автоматика, вимірювання та керування*. 2013. № 753. С. 90–99.

19. Мельник Г. Модель оценивания уровня информационных рисков в корпоративных системах. *Вісник Київського національного університету імені Тараса Шевченка. Сер. Економіка*. 2015. № 6 (171). С. 48–54.

20. Гловацький В. В. Методи оцінювання стану безпеки та загроз інформаційних ресурсів. *Зв’язок*. 2016. № 5. С. 13–16.

REFERENCES:

1. Kocziszky György (2017) Anti-corruption compliance in the enterprise's program. Strategichni perspektyvy rozvytku ekonomichnyh subyektiv v nestabilnomu ekonomichnomu seredovyshchi. pp. 164–167.

2. Kocziszky G., Veres Somosi M., Kobielieva T. (2017) Compliance risk in the enterprise. Stratehiyi innovatsiynogo rozvytku ekonomiky Ukrayiny: problem, perspektyvy, efektyvnist. Kharkiv: NTU KhPI, pp. 54–57.

3. Nagy S., Sikorska M., Pererva P. (2018) Current evaluation of the patent with regarding the index of its questionnaire. Suchsni pidhody do kreatyvnoho upravlinnya ekonomichnymy protsesamy. Kyiv: NAU, pp. 21–22.

4. Kobielieva T. O. (2020) Sutnist ta vyznachennia komplaiens-ryzyku [The essence and definition of compliance risk]. *Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI". Ekonomichni nauky*, no. 1 (3), pp. 116–121.

5. Melnyk M. O. (2017) Analiz pobudovy modeli polityky informatsiynoi bezpeky pidpryiemstva [Analysis of the construction of the information security policy model of the enterprise]. *Systemy obrobky informatsii*, no. 2(148), pp. 126–128.

6. Stepanov V. Yu. (2016) Informatsiyna bezpeka yak skladova derzhavnoi informatsiynoi polityky [Information security as a component of state information policy]. *Derzhavne budivnytstvo*, no. 2. URL: http://www.kbuapa.kharkov.ua/e-book/db/2016-2/doc/1/02.pdf.

7. Diachkov D. V. (2019) Formuvannia modeli polityky informatsiinoi bezpeky na osnovi kontseptsii hlybynnoho zakhystu [Formation of the information security policy model based on the concept of protection in depth]. *Pidpryiemnytstvo i torhivlia*, no. 25, pp. 116–121.

8. Saveleva T. V., Panasko O. M., Pryhodiuk O. M. (2018) Analiz metodiv i zasobiv dlia realizatsii ryzyk-oriientovanoho pidkhodu v konteksti zabezpechennia informatsiinoi bezpeky pidpryiemstva [Analysis of methods and means for the implementation of a risk-oriented approach in the context of ensuring the information security of the enterprise]. *Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Seriia: Tekhnichni nauky*, no. 1, pp. 81–88.

9. Babenko L. (2001) Osnovy prohramnoi inzhenerii [Fundamentals of software engineering]. Kyiv: Znannia, 269 p.

10. Hundar K., Hundar A., Yanyshevskyi D. (2000) Zashchyta ynformatsyy v kompiuternykh systemakh [Protection of information in computer systems]. Kyiv: Korneichuk, 152 p.

11.Tsehelyk H. (2018) Chyselni metody [Numerical methods]. Lviv: Vyd. tsentr LNU im. Ivana Franka, 408 p.

12. György Kocziszky, M.Veres Somosi, T.O.Kobielieva (2017) Reputational compliance. Doslidzhennia ta optymizatsiia ekonomichnykh protsesiv "Optymum–2017": tr. 13-i Mizhnar. nauk.-prakt, konf. 6-8 hrudnia 2017 r. Kharkiv: NTU "KhPI", pp. 140–143.

13. Sikorska M. (2017) Compliance service at guest services enterprises. Menedzhment rozvytku sotsialno-ekonomichnykh system u noviy ekonomitsi: materialy Mizhnar. nauk.-prakt. internet-konf. 19 zhovtnia 2017 r. Poltava: PUET, pp. 389–391.

14. Klymko T. Iu. (2015) Korporatyvnyy komplaiens yak preventyvnyy zakhid borotby z shakhraystvom [Corporate compliance as a preventive measure to combat fraud]. *Ekonomika i Finansy*, no. 6–7, p. 25.

15. Kozyreva N. A. (2015) Vnutrennyy kontrol y komplaens [Internal control and compliance]. *Vnutrennyy kontrol v kredytnoy orhanyzatsyy*, no. 1, p. 65.

16. Churubrova S. M. (2016) Polityka informatsiynoi bezpeky v systemakh informatsiyno-analitychnoho zabezpechennia pidtrymky pryyniattia orhanizatsiynykh rishen [Information security policy in information and analytical support systems for organizational decision-making]. *Problemy prohramuvannia*, no. 4, p. 97–103.

17. Zamula A. A., Severynov A. V., Korniienko M. A. (2014) Analiz modeley otsinky ryzykivv informatsiinoi bezpeky dlia pobudovy systemy zakhystu informatsii [Analysis of risk assessment models in information security for building an information protection system]. *Nauka i tekhnika Povitrianykh Syl Zbroynykh Syl Ukrainy*, no. 2 (15), pp. 133–138.

18. Harasym Yu. R., Romaka V. A., Rybiy M. M. (2013) Analiz protsesu upravlinnia ryzykamy informatsiynoi bezpeky v protsesi zabezpechennia vlastyvosti zhyvuchosti system [Analysis of the process of information security risk management in the process of ensuring the survivability of systems]. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Ser. Avtomatyka, vymiriuvannia ta keruvannia*, no. 753, pp. 90–99.

19. Melnyk H. (2015) Model otsenyvanyia urovnia ynformatsyonnykh ryskov v korporatyvnykh systemakh [Model of assessing the level of information risks in corporate systems]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Ser. Ekonomika*, no. 6 (171), pp. 48–54.

20. Hlovatsky V. V. (2016) Metody otsiniuvannia stanu bezpeky ta zahroz informatsiўnykh resursiv [Methods of assessing the state of security and threats of information resources]. *Zviazok*, no. 5, pp. 13–16.