УДК 65.011.56; 658.5.011
JEL Classification: B50, M10
DOI: 10.20535/2307-5651.22.2022.260169

Тупкало В. М.
доктор технічних наук, професор
ORCID ID: 0000-0002-6594-530X

Заплотинський Б. А.
кандидат технічних наук, доцент
ORCID ID: 0000-0002-1483-5418

Київський інститут інтелектуальної власності та права
Національного університету «Одеська юридична академія»

Tupkalo Vitalii, Zaplotynskyi Borys
Kyiv Institute of Intellectual Property and Law,
National University "Odessa Law Academy"

СТРУКТУРНИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЦИФРОВОГО ПРОЦЕСНО-ОРІЄНТОВАНОГО ПІДПРИЄМСТВА

STRUCTURAL APPROACH TO BUILDING THE DIGITAL INFORMATION SECURITY SYSTEM PROCESS-ORIENTED ENTERPRISE

На основі критичного аналізу існуючих трактувань понять «інформаційна безпека» та її складових, «кібербезпека» і «мережева безпека», викладено авторське бачення структурної моделі побудови системи інформаційної безпеки цифрового процесно-орієнтованого підприємства. Модель ґрунтується на основі комплексного системного причинно-наслідкового характеру зв'язків двох процесуальних авторських моделей: «ланцюжок створення бізнес-цінності підприємства» та «піраміда процесного менеджменту». Визначено, що ланцюжок створення бізнес-цінності підприємства – це логічна послідовність цифровізованих технологічних бізнес-процесів (ТБП) створення бізнес-цінності підприємства: залучення споживача, підготовка виробництва, виробництво товару/надання послуг, продаж товару / послуг. При цьому, під поняттям «створена бізнес-цінність підприємства» розуміється сукупність двох результатів цільового виробництва: виготовлений товар/послуга, як цінність для споживача та виручка від продажу, що надійшла на банківський рахунок продавця – цінність для підприємства. В якості моделі інструменту збору, обробки і представлення первинних облікових даних від кожного технологічного бізнес-процесу ланцюжка створення бізнес-цінності та аналітичних управлінських даних від особистих процесів управління керівників використовується система автоматизованих робочих місць (АРМ) по всім рівням піраміди процесного менеджменту. Ця система є корпоративним порталом підприємства, який має зв'язок з Internet. При цьому, під поняттям «піраміда процесного менеджменту підприємства» розуміється модель структури цифровізованого організаційного управління процесно-орієнтованого підприємства, яка є ієрархічною системою керованих по відомому управлінському циклу PDCA (плануй – організовуй – контролюй – аналізуй та впливай) внутрішніх і залежних між собою функціональних дій кожного керівника і підлеглих йому безпосередньо керівників нижнього (суміжного) рівня управління, кінцевою метою діяльності яких є вироблення управлінських рішень для безпосередньо підпорядкованих їм виконавців. Щодо пропонованої процесно-орієнтованої цифровізованої моделі управління підприємства визначено бачення моделі можливих інцидентів внутрішніх та хакерських спотворень баз даних автоматизованої системи управління підприємства. З аналізу складових цих двох моделей запропонований авторський варіант визначення поняття «Інформаційна безпека цифрового підприємства».

Ключові слова: *цифрове підприємство, цифровізована модель управління підприємства, інформаційна безпека, модель інформаційної безпеки підприємства.*

The article, based on a critical analysis of existing interpretations of the concepts of "information security" and its components, "cybersecurity" and "network security", presents the author's vision of the structural model of building an information security system of digital process-oriented enterprise. The model is based on the complex systemic causal nature of the relationship between the two procedural authorial models: "the chain of creating business value of the enterprise" and "pyramid of process management". It has been determined that the business value creation chain of an enterprise is a logical sequence of digitalized technological business processes (TBP) for creating an enterprise's business value: attracting a consumer, preparing production, producing goods / providing services, selling goods / services. At the same time, the concept of "created business value of an enterprise" means a combination of two results of targeted production: a product / service produced as a value for the consumer and sales proceeds received on the bank account of the seller – a value at the enterprise. The model of tool for collecting, processing and presenting primary accounting data from each technological business process of the business value chain and analytical management data from personal management processes is presented as a system of automated workstations (AWP) at all levels of the process management pyramid. This system is the corporate portal of the enterprise, which has a connection to the Internet. In this case, the concept of "pyramid of process management of the enterprise" means a model of the structure of digitized organizational management of process-oriented enterprise. The pyramid is a hierarchical system of internal and interdependent functional actions of each manager and subordinate managers of the lower (adjacent) level of management, managed by a well-known PDCA management cycle (plan – organize – control – analyze and influence), the ultimate goal of which is to make management decisions for performers directly subordinate to them. Regarding the proposed process-

oriented digital model of enterprise management, the vision of the model of possible incidents of internal and hacker distortions of the databases of the automated enterprise management system is defined. Based on the analysis of the components of these two models, the author's version of the definition of the concept of "Information security of a digital enterprise" is proposed.

Keywords: *digital enterprise, digitalized enterprise management model, information security, enterprise information security model.*

Вступ. Цифрова економіка, як породження Концепції «Індустрія 4.0» [1], стає сьогодні новим рушієм розвиту економіки та суспільства в цілому. З поглядом на цю новітню потребу стає актуальною проблема створення відповідної методології цифровізації сучасних підприємств, яка є визначальним базисом практичної реалізації цифрової економіки у всіх її масштабних проявах (регіональному, загальносвітовому) [2; 3]. Це, в свою чергу, породжує нову проблему – забезпечення інформаційної безпеки цифрових підприємств.

Аналіз останніх досліджень і публікацій. В контексті загальної проблеми забезпечення інформаційної безпеки різних організаційних структур існує багато публікацій, в яких автори намагаються дати варіанти визначення поняття «інформаційна безпека» та її складових «кібербезпека», «мережева безпека» [4–11]. Практично ці поняття розглядаються окремо один від одного і не дають системного (комплексного) уявлення про шляхи рішення проблеми забезпечення інформаційної безпеки цифровізованих організаційних структур в контексті співвідношення ланцюжка цих понять. Однак проведений поглиблений аналіз цих джерел дає підставу вважати, що слід погодитись з авторами роботи [4] щодо вказаного ланцюжка (див. рис. 1).

Рис. 1. Співвідношення ланцюжка понять «інформаційна безпека», «кібербезпека», «мережева безпека»

Джерело: [4]

При цьому трактування понять моделі рис.1 може бути наступним:

– *інформаційна безпека* – стан запобігання несанкціонованому доступу, використання, розкриття, спотворення, зміни, дослідження, запису або знищення інформації. Це універсальне поняття застосовується незалежно від форми, яку можуть приймати дані;

– *кібербезпека* – захищеність життєво важливих інтересів людини, суспільства, держави та окремих організацій (підприємств) під час використання інформаційного цифрового комунікативного середовища (кіберпростору), своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз цим інтересам у кіберпросторі;

– *мережева безпека* – складова поняття «кібербезпека», яка характеризує діяльність або процес щодо забезпечення захищеності глобальних та локальних телекомунікаційних мереж від несанкціонованого доступу в мережу з боку сторонніх осіб (хакерів) з ціллю порушення зберігання даних та ефективного функціонування мережі в цілому.

Слід зазначити, що в контексті актуальності проблеми забезпечення інформаційної безпеки різних організаційних структур необхідно враховувати сучасну тенденцію переходу до інжинірингу процесно-орієнтованої системи управління підприємством [12–14]. З цього приводу аналіз публікацій показує, що практично відсутній акцент на необхідність розгляду проблеми забезпечення інформаційної безпеки підприємств (*предмету дослідження*) з позицій його процесно-орієнтованої цифровізованої інформаційної моделі управління (*об'єкт дослідження*). Тобто, *об'єкт дослідження* знаходиться поза уваги.

Постановка завдання. Виходячи з вищезазначеного, можна стверджувати, що необхідні ґрунтовні дослідження щодо розробки структурної моделі забезпечення інформаційної безпеки процесно-орієнтованого цифрового підприємства. На основі критичного аналізу існуючих трактувань понять «інформаційна безпека» та її складових, «кібербезпека» і «мережева безпека», пропонується викласти авторське бачення концептуальних засад структурного моделювання системи інформаційної безпеки цифрового підприємства з позицій його процесно-орієнтованої цифровізованої інформаційної моделі управління.

Методологія. При проведенні дослідження використовувались: метод первинного спостереження з ціллю збору інформації, вивчення джерел по темі дослідження; метод системного обґрунтування пропонованих складових категорійного апарату цифрового менеджменту; метод структурно-логічної формалізації з ціллю наочного представлення методологічних складових цифровізованої процесно-орієнтованої моделі управління підприємства та моделі можливих інцидентів внутрішніх та хакерських спотворень баз даних підприємства.

Результати дослідження. Згідно поставленої мети необхідно, в першу чергу, звернути увагу на сформоване у фаховому середовищі співвідношення ланцюжка понять «інформаційна безпека», «кібербезпека», «мережева безпека» (рис. 1) [4].

В контексті поняття «процесно-орієнтована цифровізована модель управління підприємства» (*об'єкт дослідження*) пропонується наступне визначення.

Визначення 1. Цифрове підприємство (Digital Enterprise) – організація, яка використовує інформаційні технології (ІТ) у всіх сферах своєї діяльності згідно моделі системи (ланцюжка) цифровізованих технологічних бізнес-процесів (ТБП) створення бізнес-цінності підприємства: залучення споживача, підготовка виробництва, виробництво товару/надання послуг, продаж товару/послуг. В якості інструменту збору, обробки і представлення первинних облікових даних від технологічних процесів (ТП) кожного ТБП та аналітичних управлінських даних від особистих про-

цесів управління (ПУ) керівників використовується система автоматизованих робочих місць (АРМ) по всім рівням піраміди процесного менеджменту. Всі АРМ об'єднані у корпоративний портал підприємства, який має зв'язок з Internet. При цьому, під поняттям «створена бізнес-цінність підприємства» розуміється сукупність двох цільових результатів: виготовлений товар/надана послуга, як цінність для споживача та виручка від продажу, що надійшла на банківський рахунок продавця – цінність для підприємства. Згідно даному визначенню, структурована по рівням менеджменту процесно-орієнтована цифровізована модель управління підприємства (цифровізована піраміда процесного менеджменту) представлена на рис. 2.

Згідно моделі рис. 2 можна стверджувати, що корпоративна мережа АРМів з точки зору побудови системи кібербезпеки підприємства є комплексом з окремих чотирьох рівневих мереж АРМів. За рівнем менеджменту в автоматизованій системі кібербезпеки підприємства (АСКП) ці рівневі мережі можуть бути сформовані так:

– АРМи вищих керівників – генерального директора, членів наглядової ради тощо;

– АРМи заступників директора по видам господарської діяльності, які є центрами стратегічної відповідальності (комерційний директор, директор з виробництва, фінансовий директор, директор з організаційного розвитку);

– АРМи керівників середнього та нижчого рівнів управління (начальники відділів, окремих служб та ін.);

– АРМи виконавців робіт технологічних процесів ланцюжка створення споживчої цінності, які безпосередньо створюють БД потоків первинних даних.

При цьому, під поняттям «цифровізована піраміда процесного менеджменту підприємства» розуміється модель структури цифровізованого організаційного управління процесно-орієнтованого підприємства, яка є ієрархічною системою керованих по відомому управлінському циклу PDCA (плануй → організовуй → контролюй → аналізуй та впливай) внутрішніх і залежних між собою функціональних дій кожного керівника і підлеглих йому безпосередньо керівників нижнього (суміжного) рівня управління, кінцевою метою діяльності яких є вироблення управлінських рішень для безпосередньо підпорядкованих їм виконавців.

В контексті Визначення 1 слід зауважити, що інформація, яка створюється в системі (ланцюжку) бізнес-процесів створення бізнес-цінності підприємства, представляє певну ціну. Тому сам факт отримання інформації зловмисником в інтересах конкурентів підприємства приносить йому певний дохід. Звідси головна мета зловмисника – отримання інформації про склад, стан і діяльність об'єкта конфіденційних інтересів (про вироби (товари/послуги), бізнес-проекти, рецепти, технології тощо). Крім того, з корис-

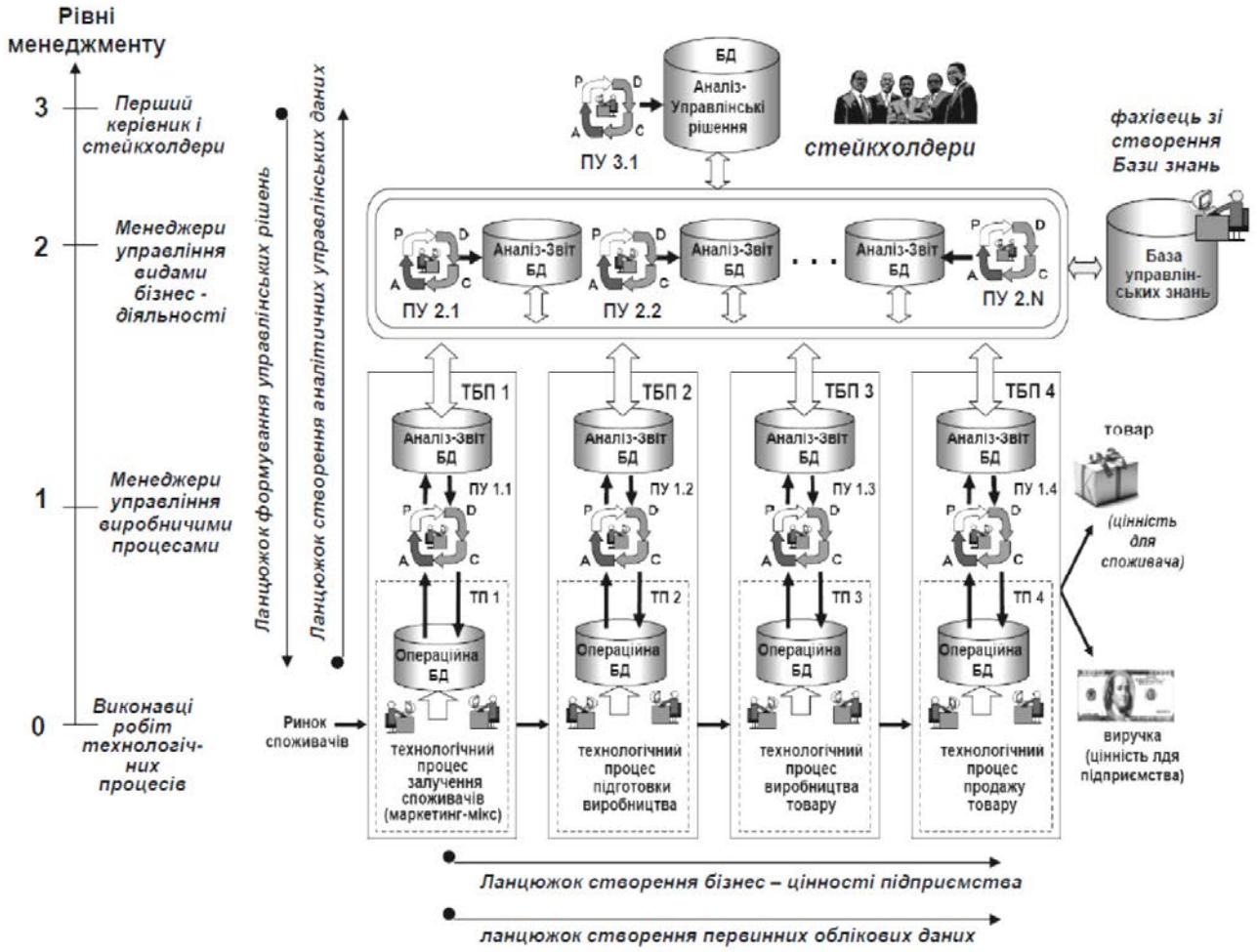

Рис. 2. Цифровізована процесно-орієнтована модель управління підприємства (авторська модель)

ною метою можливе і внесення певних спотворень до складу інформації, що циркулює на об'єкті конфіденційних інтересів. Така дія може призвести до дезінформації керівництва підприємства щодо облікових даних і результатів вирішення деяких бізнес-завдань. В кінцевому рахунку, це впливає на достовірність оцінки ефективності певних сфер діяльності підприємства з боку керівництва в цілому.

Більш небезпечною метою спотворення інформації є знищення накопичень інформаційних масивів у документальній цифровій формі (баз даних) та програмних продуктів зі збирання, обробки та подання аналітичної інформації для прийняття управлінських рішень керівництвом підприємства. Фактично, в цьому випадку здійснюється зловмисне втручання в масштабі автоматизованої системи управління підприємства (АСУП). У зв'язку з цим для підприємства дедалі більшого значення набуває створення структурованої по всім технологічним і управлінським бізнес-процесам моделі організації ефективної системи інформаційної безпеки як в організаційному, так і програмно-технічному плані.

Виходячи з вищезазначеного, для побудови збалансованої структурної моделі інформаційної безпеки підприємства спочатку необхідно провести аналіз ризику в області безпеки інформаційних потоків підприємства по всій системі бізнес-процесів піраміді менеджменту і створити модель можливих інцидентів внутрішніх та хакерських спотворень баз даних підприємства. Концептуально така структурна модель представлена на рис. 3. В контексті цієї моделі можна виділити низку ймовірних джерел загроз інформаційній безпеці бізнес-середовищу сучасного підприємства:

– порушення встановлених регламентів збору, обробки та передачі інформації;

– навмисні дії персоналу інформаційних систем;

–не навмисні помилки персоналу інформаційних систем;

– помилки в проектуванні інформаційних систем (АСУП).

Аналізуючи причинно-наслідковий зв’язок моделей, рис. 2 і 3, слід зазначити, що сутність і новизна моделі рис. 2 полягає в реалізації принципу «не треба класти яйця в одну корзину» щодо розміщення всієї сукупності корпоративної бази даних і знань фізично на одному загальному сервері підприємства, який має одну IP-адресу.

Виходячи з вищезазначеного пропонується наступне визначення.

Визначення 2. Система інформаційна безпека цифрового підприємства – комплекс заходів організаційного та технічного характеру щодо розосередження загальної бази корпоративних даних і знань по окремим рівневим серверам рівневих первиних баз даних, аналітико-управлінських баз даних та бази знань підприємства згідно створеної моделі піраміди процесного менеджменту підприємства з ціллю забезпечення надійності захисту збереження комерційної й управлінської інформації та її ключових елементів від ймовірних зовнішніх (кібератак) і внутрішніх загроз крадіжок та спотворення, знищення накопичень інформаційних масивів на цифрових носіях та програмних продуктів зі збирання, обробки та подання аналітичної інформації для прийняття об’єктивних управлінських рішень керівництвом підприємства.

Висновки. На відміну від звісної поширеної моделі побудови АСКП на основі формування однорангової клієнт-серверної мережі АРМів шляхом розміщення всієї сукупності корпоративної бази даних і знань фізично на одному загальному сервері підприємства, який має одну IP-адресу, новизна пропонованої моделі полягає в реалізації одного з можливих шляхів мереже-

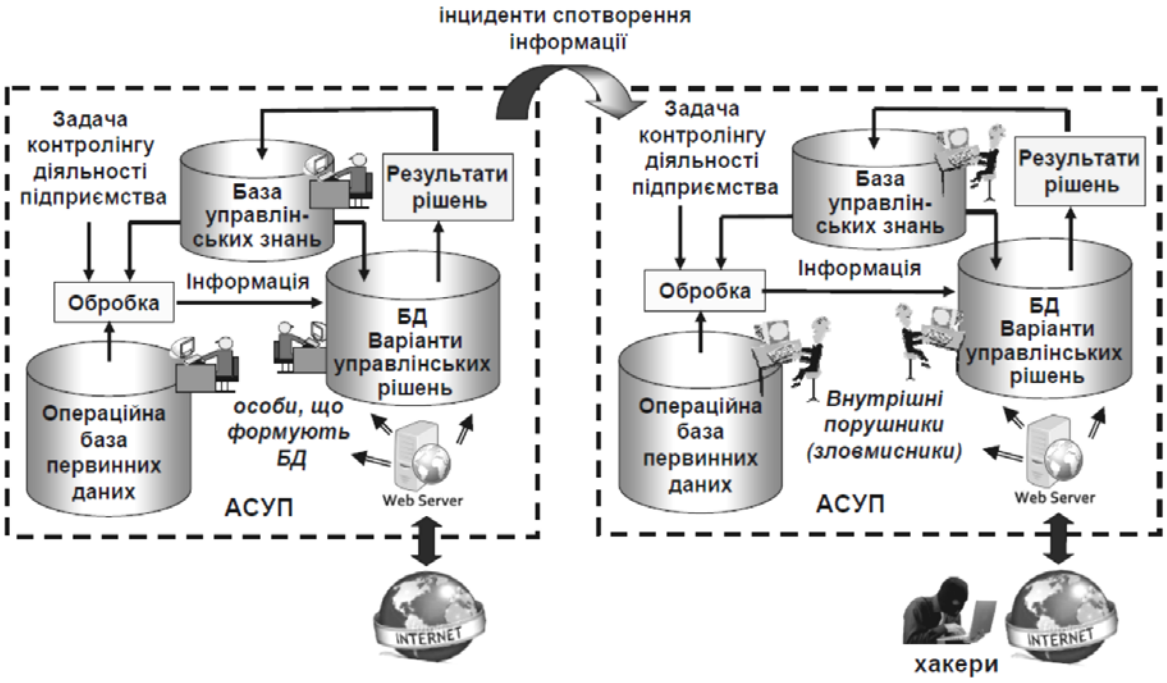

Рис. 3. Структурна модель можливих інцидентів внутрішніх та хакерських спотворень баз даних підприємства (авторська модель)

вої безпеки, заснованого на принципі розподілення «не треба класти яйця в один кошик». Тобто, формування загальної локальної мережі АРМів підприємства відбувається як комплекс окремих рівневих мереж згідно класифікації АРМів за рівням управління. При цьому кожна рівнева мережа має свій окремий сервер з відповідною IP-адресою. Таким чином, розглянутий в статті концептуальний структурний підхід щодо моделювання системи інформаційної безпеки цифрового процесно-орієнтованого підприємства дає можливість проведення поглибленої її оцінки на кожному з рівнів корпоративної мережі АРМів піраміди процесного менеджменту підприємства (збільшується глибина діагностування місць виникнення інцидентів внутрішніх та хакерських спотворень баз даних).

Враховуючи ймовірність джерел загроз інформаційній безпеці бізнес-середовищу сучасного підприємства в наслідок помилок при проектуванні його АСУП, можна вважати, що перспективою подальших досліджень може бути усунення таких помилок шляхом використання технології комплексного синтезу системи бізнес-процесів цифрового підприємства (піраміди процесного менеджменту) на основі врахування вимоги бієктивності відображення (трансформації) ієрархічної системи бізнес-цілей підприємства в ієрархічну структуру його центрів управлінської відповідальності.

Література:

1. Антонов В. Г., Самосудов М. В. Проблемы и перспективы развития цифрового менеджмента. URL: https://e-management.guu.ru/jour/article/view/16 (дата звернення: 11.05.2022).

2. Шушунова Т. Н., Вакуленко В. Ф., Фролова А. В. Современные тренды и перспективы развития менеджмента в условиях цифровой трансформации. URL: https://cyberleninka.ru/article/n/sovremennye-trendy-i-perspektivy-razvitiya-menedzhmenta-v-usloviyah-tsifrovoy-transformatsii/viewer (дата звернення: 11.05.2022).

3. Баранов О.А. Інтернет речей (IoT): мета застосування та правові проблеми. *Інформація і право*. 2018. № 2(25). С. 31–44. URL: http://ippi.org.ua/sites/default/files/5_9.pdf (дата звернення: 11.05.2022).

4. Козлова О. Ю., Кононович В. Г., Кононович І. В., Романюков Л. М., Тимошенко М. Г. Динамічні властивості процесів забезпечення кібербезпеки на прикладі аудиту кібербезпеки. *Інформатика та математичні методи в моделюванні.* 2017. Т. 7. № 3. С. 205–212.

5. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельниц. нац. ун-ту. Сер. : Екон. науки.* 2010. Т. 2. № 2. С. 32–35.

6. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. Москва : Академия, 2008. № 3. 336 с.

7. Давидюк Т.В., Боримська К.П. Позиціонування обліково-аналітичного забезпечення економічної безпеки підприємства в навчальних планах фахівців напряму підготовки «Облік і аудит». *Економіка: реалії часу.* 2013. № 3(8). С. 83–90.

8. Цаль-Цалко Ю. С., Мороз Ю. Ю. Облікова політика підприємства та її кібербезпека / Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства: збірник наукових праць. ПП «Рута». Т. IV, І. 2017. С. 8–11.

9. Що таке безпека мережі? URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/bezopasnost-seti/ (дата звернення: 11.05.2022).

10. Герасимов В. В., Хисаева Г. Ф., Гарипов И.М. Система обнаружения вторжений как важнейший элемент системы информационной безопасности корпоративной сети предприятия. Ассоциация научных сотрудников «Сибирская академическая книга». 2019. С. 303–307.

11. Сетевая безопасность. 2015. URL: https://habr.com/ru/company/hpe/blog/261913/ (дата звернення: 11.05.2022).

12. Швиданенко Г. О., Приходько Л. М. Оптимізація бізнес-процесів : навч. посіб. Київ : КНЕУ, 2012. 487 с.

13. Тупкало В. М. Бізнес-інжиніринг сучасних процесно-орієнтованих підприємств : монографія. Київ : ДУТ, 2016. 281 с.

14. Мальцев С. В. Процессный подход к управлению: теория и практика применения. URL: http://www.svmal.ru/info_2.html (дата звернення: 02.01.2022).

References:

1. Antonov V. G., Samosudov M. V. (2022). Problems and prospects for the development of digital management. Available at: https://e-management.guu.ru/jour/article/view/16 (accessed 11 May 2022).

2. Shushunova T. N., Vakulenko V. F., Frolova A. V. (2022). Modern trends and prospects for the development of management in the context of digital transformation. Available at: https://cyberleninka.ru/article/n/sovremennye-trendy-i-perspektivy-razvitiya-managementa-v-usloviyah-tsifrovoy-transformatsii/viewer (accessed 11 May 2022).

3. Baranov O. A. (2018). Internet of Speech (IoT): metastases and legal problems. *Information and Law*, no. 2(25), pp. 31–44. Available at: http://ippi.org.ua/sites/default/files/5_9.pdf (accessed 11 May 2022).

4. Kozlova O. Yu., Kononovich V. G., Kononovich I. V., Romanyukov L. M., Timoshenko M. G. (2017). Dynamic power of cybersecurity processes in the application of cybersecurity audit. Informatics and mathematical methods in modeling: international journal category B. ONPU. T. 7, no. 3, pp. 205–212.

5. Sorokivska O. A., Gevko V. L. (2010). Informational business security: new threats and prospects. *Visnik Khmelnytsky. nat. un-tu. Ser.: Econ. Sciences*. T. 2, no. 2, pp. 32–35.

6. Melnikov V. P., Kleimenov S. A., Petrakov A. M. (2008). Information security and information protection. Moscow: Academy, no. 3, 336 p.

7. Davidyuk T. V., Borimska K. P. (2013). The position of oblikovo-analytical security of economic security of business in the initial plans of fakhivtsiv directly preparing "Oblik i audit". *Economics: realities of the hour*. Scientific journal, no. 3(8), pp. 83–90.

8. Tsal-Tsalko Yu. S., Moroz Yu. Yu. (2017). General business policy and cyber security / Shape, analysis and control in the minds of modern concepts of managing the economic potential and market variety of business: a collection of scientific practices. PE "Ruta". T. IV, I, pp. 8–11.

9. What is the safety of merezhi? Available at: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/bezopasnost-seti/ (accessed 11 May 2022).

10. Gerasimov V. V., Khisaeva G. F., Garipov I. M. (2019). Intrusion detection system as an essential element of the information securi. Association of Research Fellows "Siberian Academic Book", pp. 303–307.
11. Network security (2015). URL: https://habr.com/ru/company/hpe/blog/261913/ (accessed 11 May 2022).
12. Shvidanenko G. O., Prikhodko L. M. (2012). Optimization of business processes: Navch. posib. Kyiv: KNEU, 487 p.
13. Tupkalo V. M. (2016). Business engineering of modern process-oriented enterprises: monograph. GUT, 281 p.
14. Maltsev S. V. Process approach to management: theory and practice of application. Available at: http://www.svmal.ru/info_2.html (accessed 11 May 2022).