УДК 658.012.4:621

Тупкало В. М.
д-р. техн. наук, професор
Київський університет інтелектуальної власності та права
м. Київ, Україна
ORCID: 0000-0002-6594-530X;
Ярмолатій А. В.
викладач кафедри кібербезпеки, інформаційних технологий та економіки
Київський університет інтелектуальної власності та права
м. Київ, Україна
ORCID: 0000-0002-4168-4002

МЕТОДОЛОГІЧНІ ЗАСАДИ ПРОЦЕСНО-ОРІЄНТОВАНОГО ПІДХОДУ ДО ВПРОВАДЖЕННЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКА ПІДПРИЄМСТВА

В контексті проблеми забезпечення інформаційної безпеки (кібербезпеки) підприємств та установ критичної інфраструктури актуальною стає задача розробка системології щодо впровадження системи менеджменту інформаційної безпеки (СМІБ, англ. Information Security Management System, ISMS) на засадах системного процесно-орієнтованого підходу [1, 2]. У доповіді на основі критичного аналізу відомих наукових дослідженнях (публікаціях) вітчизняних та зарубіжних вчених зроблено висновок про необхідність подальших ґрунтовних досліджень в цьому напрямку. В першу чергу це стосується розв'язання задачі виявлення множини об'єктів інформаційної безпеки у системі управлінських і технологічних процесів підприємств. Оскільки ця система належить до категорії «складна система», [3] тому актуальним стає дослідження системології систем інформаційної безпеки підприємства, як системного об'єднання інформаційних та організаційних (персонал, піраміда менеджменту) його ресурсів. Мета дослідження – обґрунтування запропонованого авторського системного процесно-орієнтованого підходу та комплексної моделі побудови СМІБ підприємства з позиції фундаментальної теорії організаційного управління.

З цього приводу в основу рішення задачі синтезу покладено два логічно пов'язаних концептуальних тверджень: – СМІБ є невід'ємною складовою частиною загальної системи менеджменту підприємства; – а об'єктами інформаційного захисту (кіберзахисту) є інформаційні активи підприємства A_{IT}, до яких належать апаратні та програмні компоненти бізнес-процесів інформаційної системи підприємства (інформаційного поля підприємства), що забезпечують виконання його цільових завдань зі створення споживчої цінності. Враховуючи, що стандарт ДСТУ ISO/IEC 27000:2019 визначає інформаційну безпеку як «збереження конфіденційності, цілісності та доступності інформації...» [4], рішення задачі забезпечення інформаційної безпеки підприємства можна представити у вигляді моделі рис.1.

На першому етапі проводиться виділення та опис у відповідній нотації всієї системи бізнес-процесів підприємства з метою виявлення інформаційних активів АІТ інформаційного поля, як об'єктів подальшого аудиту стану інформаційної безпеки. На другому етапі відбувається процес послідовної оцінки можливості інформаційних загроз для АІТ на рівні окремих ІТ-ресурсів, на рівні безпеки інфраструктури окремих організаційних структур підприємства і в цілому – всього інформаційного поля за напрямками (видами) господарської діяльності підприємства.

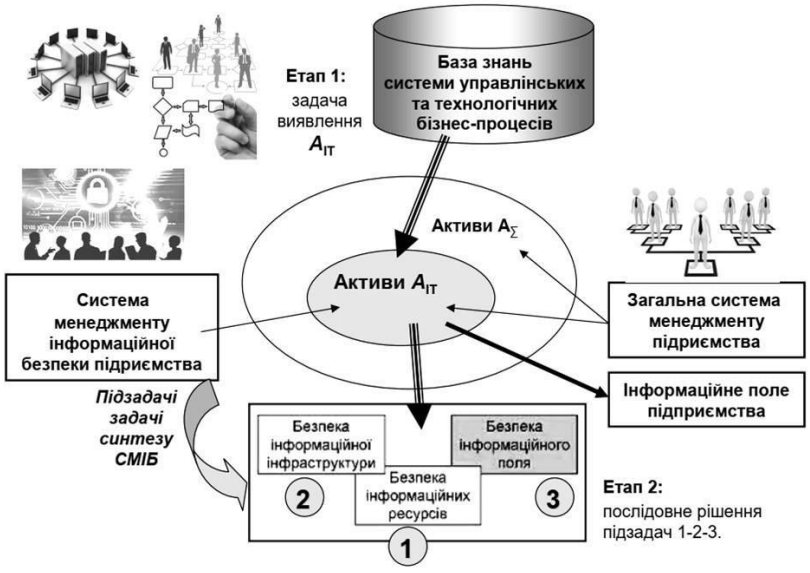

Рисунок 1 – Структура та етапи рішення задачі забезпечення інформаційної безпеки підприємства (авторська модель)

У контексті моделі Рис.1 запропоновано авторське визначення поняття «Інформаційне поле підприємства – це скоординована багаторівнева процесно-орієнтована структура, що акумулює результати комунікаційної діяльності підприємства за допомогою конкретних компонентів системи інформації та зв'язку, яка породжується системою бізнес-процесів і має відповідну форму та носії її операційного зберігання інформації.

Слід зазначити, що $A_{ІТ}$ є підмножиною сумарних активів підприємства $A_{\sum}$ і вирішують задачу недопущення погіршення стану інформаційної захищеності тієї частки сумарних активів, яка безпосередньо використовується у фінансово-господарській діяльності з метою отримання прибутку. При цьому стверджується, що сформований таким чином системний опис у формі бази знань (БЗ) про інформаційне поле підприємства слід розглядати як первинний актив множини $A_{ІТ}$.

Результат рішення задачі синтезу: на основі запропонованої моделі піраміди (дерева) процесного менеджменту СМІБ сформована низка системно пов'язаних визначень понятійного апарату та структурних моделей вирішення комплексної задачі забезпечення інформаційної безпеки підприємства. З цього приводу у доповіді зазначено, що побудова системи процесно-орієнтованого управління підприємством неможлива без формалізованого опису його діяльності, і передусім системи бізнес-процесів. Такий опис сприяє вирішенню крос-функціональних проблем у підприємстві, пов'язаних з наявністю перешкод між окремими структурними підрозділами, даючи змогу ретельно розібратися в усіх нюансах його діяльності, і насамперед у бізнес-процесах, створює основу для аналізу та вдосконалення бізнес-процесів, організаційної структури та інших підсистем підприємства.

Саме модель бізнесу виступає умовою, необхідною як для побудови системи процесно-орієнтованого управління підприємством, так і для процесно-орієнтованого впровадження корпоративних інформаційних систем. У цьому плані сьогодні виник і стрімко розвивається новий інноваційний напрямок розвитку теорії організаційних систем – процесно-орієнтований бізнес-інжиніринг. Прикладною складовою процесно-орієнтованого бізнес-інжинірингу є розробка та впровадження ефективних мов (моделей) і способів системного опису бізнес-процесів підприємств. Виходячи з цього твердження, проведений аналіз існуючих мов (способів) моделювання бізнес-процесів і їх нотацій IDEF0, IDEF3, ARIS, BPMN показує [5], що істотним чинником гальмування розвитку системного процесно-орієнтованого підходу до створення та удосконаленні систем менеджменту інформаційної безпеки підприємств є відсутність єдиних методологічних поглядів (стандарту) на формати мов графічного опису бізнес-процесів, що склалися на даний момент. Про це, зокрема, красномовно свідчить, наприклад, відсутність відповідних рекомендацій у серії міжнародних стандартів ISO/IEC 27000 [4] щодо створенні систем менеджменту інформаційної безпеки організацій. В контексті цього твердження викладені базові засади авторської мови структурного синтезу системи бізнес-процесів підприємств, яка дозволяє в повній мірі виявити інформаційні активи підприємства $A_{ІТ}$ інформаційного поля підприємства [5]. Однією з принципових відмінностей нотації авторської мови є введення поділу загальної сутності «Документ» на два види: «Паперовий документ» і «Електронний документ», а сутність «Виконавець функціональної дії» доповнено двома сутностями: «Посадова особа, що використовує автоматизовану інформаційну систему підприємства» і «Посадова особа, що є центром відповідальності за введення в інформаційну систему підприємства первинних даних». Із методичної точки зору зазначена відмінність дає змогу при синтезі системи управління підприємством і, зокрема, системи менеджменту інформаційної безпеки (СМІБ) точно відобразити модель інформаційного поля по горизонталі та вертикалі піраміди процесного менеджменту. Зрештою це дозволяє точно визначити функціональні права і відповідальність конфіденціального характеру щодо розподілу прав доступу до інформаційних баз даних посадових осіб в інформаційному середовищі підприємства, об'єктивно виявити вимоги до моделі та ресурсного складу СМІБ.

Наукова новизна одержаних результатів полягає в тому, що на основі запропонованої моделі піраміди (дерева) процесного менеджменту СМІБ сформована низка системно зв'язаних визначень понятійного апарату та структурних моделей щодо рішення комплексної задачі забезпечення інформаційної безпеки підприємства.

У контексті проблеми розвитку системології інформаційної безпеки підприємств подальший розвиток теми статті бачиться у пошуку дієвого інструменту наочного опису системи управлінських і технологічних бізнес-процесів підприємств з метою виявлення критичних інформаційних активів.

Список використаних джерел

1. Загоруйко Л.В., Мартьянова Т.А., Скирда А.В. Моделі аналізу ризику безпеки інформаційних технологій: збірник наукових праць «Методи та системи оптико-електронної і цифровфої обробки зображень та сигналів». 2021. С. 16-19.

2. Лисецький Ю.М., Калбазов Д.Й. Підходи до забезпечення інформаційної безпеки. Математичні машини і системи. № 4. 2023. С. 26-32.

3. Складна система. URL: https://uk.wikipedia.org/wiki/Складна_система (дата звернення: 30.03.2024).

4. ISO/IEC 27000 family – Information security management systems [Electronic resource]. URL: https://ostec.blog/en/general/first-steps-iso-27000/ (дата звернення: 30.03.2024).

5.Tupkalo V., Zaplotynskyi B. Fundamentals of information security management system engineering of modern process-oriented enterprises: monograph. Kyiv: KUIPL, 2024. 81 p. [E-mail resource]. Issued in the Lambert Academic Publishing, www.lap-publishing.com