УДК 658.012.4:621 **Тупкало В. М.**
д-р. екон. наук, професор
завідувач кафедри кібербезпеки, інформаційних технологій та економіки
Київський інститут інтелектуальної власності та права
Національного університету «Одеська юридична академія»,
м. Київ, Україна
ORCID: 0000-0002-6594-530X

ПІДХІД ДО МОДЕЛЮВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЦИФРОВОГО ПРОЦЕСНО-ОРІЄНТОВАНОГО ПІДПРИЄМСТВА

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». Практично ці поняття носять виключно загальний інформаційно - технологічний або дискусійно-філософський характер і розглядаються окремо один від одного, що не дає системного (комплексного) уявлення про шляхи рішення проблеми забезпечення інформаційної безпеки (кібербезпеки, мережевої безпеки) цифровізованих організаційних структур в контексті співвідношення ланцюжка цих понять. Крім того, необхідно враховувати сучасну тенденцію переходу до інжинірингу процесно-орієнтованої системи управління підприємством [1]. З цього приводу аналіз публікацій показує, що практично відсутній акцент на необхідність розгляду проблеми забезпечення інформаційної безпеки підприємств (*предмету дослідження*) з позицій його прецесно-орієнтованої цифровізованої інформаційної моделі управління (*об'єкт дослідження*). Тобто, *об'єкт дослідження* знаходиться поза уваги.

На основі критичного аналізу існуючих трактувань понять «інформаційна безпека» та її складових 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» [2]. Визначено, що ланцюжок створення бізнес-цінності підприємства – це логічна послідовність цифровізованих технологічних бізнес-процесів створення бізнес – цінності підприємства: залучення споживача/замовника, підготовка виробництва, виробництво товару/надання послуг, продаж товару/послуг. 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 по всім рівням піраміди процесного менеджменту. Ця система є корпоративним порталом підприємства, який має зв'язок з Internet. 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 основу побудови цієї моделі покладено трирівневу управлінську модель П. Друкера [3].

З переліченого вище слід зауважити, що інформація, яка створюється в системі (ланцюжку) бізнес-процесів створення бізнес – цінності підприємства, представляє певну цінність. Звідси головна мета зловмисника (хакера) - отримання інформації про склад, стан і діяльність об'єкта конфіденційних інтересів (про вироби (товари/послуги), бізнес-проекти, рецепти, технології тощо). Крім того, з корисною метою можливе і внесення певних спотворень до складу інформації, що циркулює на підприємстві.

Відносно пропонованої прецесно-орієнтованої цифровізованої моделі управління підприємства визначено бачення моделі можливих інцидентів внутрішніх та хакерських спотворень баз даних автоматизованої системи управління підприємства, що дає можливість виділити низку ймовірних джерел загроз інформаційній безпеці бізнес-середовищу сучасного підприємства:

− порушення встановлених регламентів збору, обробки та передачі інформації;

− навмисні дії персоналу щодо порушення нормального функціонування окремих інформаційних підсистем підприємства;

- ненавмисні помилки персоналу інформаційних систем;

− помилки в проектуванні інформаційних систем (АСУП).

Такі зазначені дії можуть призвести до дезінформації керівництва підприємства щодо облікових даних і результатів вирішення певних бізнес-завдань. В кінцевому рахунку, це впливає на достовірність оцінки ефективності певних сфер діяльності підприємства з боку керівництва в цілому.

Структурна модель можливих інцидентів внутрішніх та хакерських спотворень баз даних підприємства представлена на рис.1.

Рисунок 1 - Структурна модель можливих інцидентів внутрішніх та хакерських спотворень баз даних підприємства
Джерело: складено автором

Виходячи з попереднього, для побудови збалансованої структурної моделі інформаційної безпеки підприємства запропоновано алгоритм дій: 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.

Треба зазначити, що у контексті сутності структурної моделі можливих інцидентів внутрішніх та хакерських спотворень баз даних підприємства виникає актуальна методологічна задача – створення інструментарію виділення, композиції та опису бізнес-процесів з максимальною можливістю виявлення інформаційних потоків і мережі баз даних цифровізованої системи менеджменту підприємства, а також однозначного встановлення в бізнес-процесах осіб, які є центрами одноосібної відповідальності за формування та забезпечення цілісності системи баз даних підприємства.

З аналізу складових вищезазначених моделей пропонується авторський варіант визначення наступних понять.

Цифрове підприємство (Digital Enterprise) — організація, яка використовує інформаційні технології у всіх сферах своєї діяльності згідно моделі системи (ланцюжка) цифровізованих технологічних бізнес-процесів (ТБП) створення бізнес – цінності підприємства. В якості інструменту збору, обробки і представлення первинних облікових даних від технологічних процесів кожного ТБП та аналітичних управлінських даних від особистих процесів управління 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.

Інформаційна безпека цифрового підприємства – комплекс заходів організаційного та технічного характеру по піраміді процесного менеджменту підприємства, спрямованих на збереження та захист 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.

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 на основі врахування вимоги бієктивності відображення (трансформації) ієрархічної системи бізнес - цілей підприємства в ієрархічну структуру його центрів управлінської відповідальності.

Література:

1. Швиданенко Г. О., Приходько Л. М. Оптимізація бізнес-процесів : навч. посіб. Київ : КНЕУ, 2012. 487 с.
2. Тупкало В.М. Бізнес – інжиніринг сучасних процесно – орієнтованих підприємств: монографія. Київ: ДУТ, 2016. 281 с.
3. Друкер, Питер, Ф. Энциклопедия менеджмента. «ИД «Вильямс», 2004. 432 с.