Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка» (Україна)
Навчально-науковий інститут фінансів,
економіки, управління та права
Батумський державний університет імені Шота Руставелі (Грузія)
Університет BIT-АП (Індія)
Державна установа «Інститут економіки
природокористування та сталого розвитку
Національної академії наук України» (Україна)
Державна установа «Інститут економіки та прогнозування Національної академії наук України» (Україна)

СУЧАСНА ЕКОНОМІЧНА НАУКА: ТЕОРІЯ І ПРАКТИКА

Матеріали XII Всеукраїнської науково-практичної Інтернет-конференції з міжнародною участю 10 листопада 2022 року

Полтава 2022

аналізувати наявні проблеми, а саме: можливість розвитку соціально-економічної системи; вплив основних макроекономічних показників на обсяги ВВП та на обсяги капіталовкладень; співвідношення індивідуального споживання та заощаджень; рівень коливань між українською і світовою економікою.

Література

1. Економічна кібернетика : підручник.Донецьк : ЮгоВосток, 2014. 454 с.
2. Кузьменко О.К., Кострубяк І.О. Прогностична модель розвитку ринкових послуг. Modern research in world science‖(June 12-14, 2022) SPC―Sci-conf. com. ua‖, Lviv, Ukraine. 2022. p. 1582–1588. URL https://www.researchgate.net/profile/M-Rumiantsev/publication/361865011_MODERN-RESEARCH-IN-WORLD-SCIENCE-12-140622/links/62c91c3d3bbe636e0c4ded01/MODERN-RESEARCH-IN-WORLD-SCIENCE-12-140622.pdf#page=1582.
3. Лапач С.Н. Статистика в науке и бизнесе / С.Н. Лапач, А.В. Чубенко, П.Н. Бабич. – К. : МОРИОН, 2002. – 640 с.
4. Математическая статистика : учебник М. : Высш. школа, 1981. 371 с.
5. Моделі й методи соціально-економічного прогнозування : [Гаєць В., Клебанова Т., Іванов В. та ін.] підручник. – Харьків : Вид-во ХДЕУ, 2003. – 270 с.
6. Фатхутдінов Р.А. Управління конкурентоздатністю організації : Навчальний посібник. – 4-е вид. – К. : Ексмо, 2015. – 544 с.
7. Федорович Р. В. Маркетинговий аналіз кон'юнктури ринку. Галицький економічний вісник. 2009. № 2. С. 47-52.
8. Яренко А.В. Систематизація кількісних методів прогнозування кон'юнктури ринку в маркетингових дослідженнях. ВІСНИК КНУТД. – №3 (87), 2015. URL : https://knutd.edu.ua/publications/pdf/Visnyk/2015-3/11_18.pdf.

УДК 658

Кузьменко О.К., к.е.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
Дюдюк А.І.
Технічний університет у Ліберці, Чехія

МОДЕЛЮВАННЯ ПРОЦЕСІВ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ТЕОРІЇ ГРАФІВ І МЕТОДОЛОГІЇ IDF0

Система захисту інформації містить у собі такі теорії, як теорія ймовірностей і випадкових процесів; теорія графів, автоматів та мереж Петрі; теорія нечітких множин; теорії ігор та конфліктів; теорія катастроф; еволюційне моделювання; формально-евристичний підхід; ентропійний підхід. При цьому,

науковцями пропонується ще використовувати методи моделювання, які засновані на неформальній теорії систем, таких як методи структурування, методи оцінювання та методи пошуку оптимальних рішень.

Враховуючи [1], систему захисту інформації представимо у вигляді орієнтованого графа. У цьому графі, нехай, вершини – це компоненти інформаційної системи, а ребра – інформаційні потоки між ними. Таким чином, сформована матриця суміжності та інцидентності дозволить визначити компоненти інформаційної системи, які обробляють інформацію різних рівнів конфіденційності з метою подальшого посилення захисту від потенційних загроз інформаційній безпеці.

Для моделювання системи захисту інформації, з точки зору поточного опису процесів, пропонуємо використовувати методології IDEF [1]. Методології IDEF – це технологія опису бізнес-процесів як множини взаємозалежних дій або функцій. Отже, цей підхід дозволить провести передпроєктне дослідження процесів системи з необхідним рівнем деталізації для подальшого виявлення «вузьких» місць і розробити заходи для реінжинірингу відповідних процесів.

Процес забезпечення інформаційної безпеки розіб’ємо на підпроцеси: аналіз вхідних даних, розподіл за рівнями захисту інформації, усунення загроз, обробка інформації засобами для захисту інформації. Далі, у рамках методології IDEF функціонування системи захисту інформації, сформуємо контекстну діаграму в нотації IDEF0, що дозволить описати логічні відносини між окремими процесами системи (рис. 1).

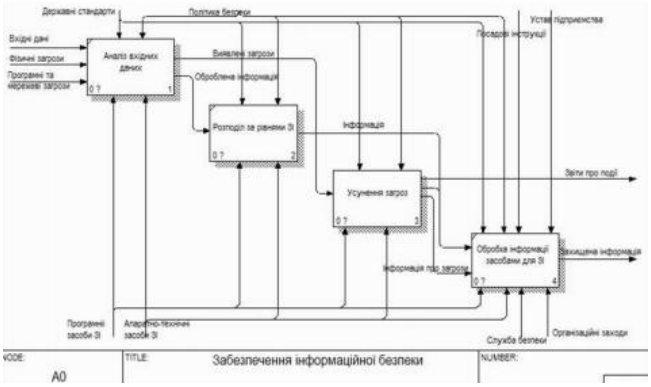

Рисунок 1. Діаграма IDEF0 «Забезпечення інформаційної безпеки»

З точки зору розробки системи захисту інформації найбільш проблемним є процес «Усунення загроз» (рис. 2). Цей процес містить наступні підпроцеси: класифікація загроз за категоріями, розробка системи захисту інформації, реалізація системи захисту інформації, планові перевірки для виявлення загроз.

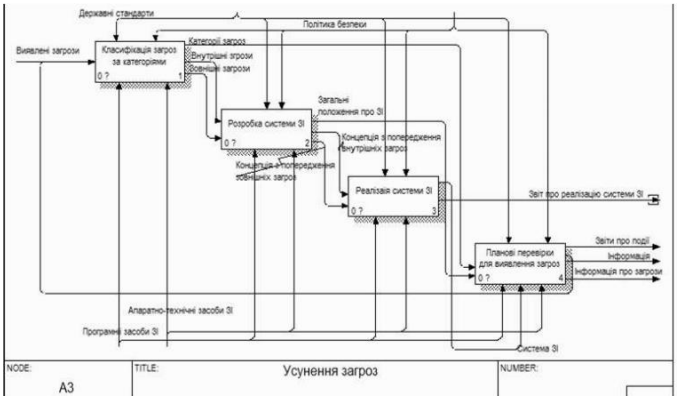

Рисунок 2. Діаграма IDEF0 «Усунення загроз»

Розглянемо декомпозицію процесу «Розробка системи захисту інформації» із використанням теорії графів, а саме моделі системи захисту з повним перекриттям. Отже, модель системи захисту з повним перекриттям може бути представлена у вигляді трьох множин: множини загроз $\mathrm{T} = \{t_i\}$, множини об'єктів захисту $\mathrm{O} = \{\mathrm{o}_j\}$, множини механізмів захисту $\mathrm{M} = \{\mathrm{m}_k\}$. Тобто систему захисту інформації можна зобразити як тридольний граф $\{\mathrm{T}, \mathrm{O}, \mathrm{M}\}$ (1) [2]. Отже, враховуючи математичну модель (1) розіб'ємо процес «Розробка системи захисту інформації» на наступні підпроцеси (рис. 3): визначення актуальних загроз – на виході отримуємо множину загроз $\mathrm{T} = \{t_i\}$; визначення інформаційних ресурсів для захисту – на виході отримуємо множину об'єктів захисту $\mathrm{O} = \{\mathrm{o}_j\}$; визначення механізмів захисту інформації – на виході отримуємо механізмів захисту $\mathrm{M} = \{\mathrm{m}_+\}$; розробка документів, регламентуючих захист інформації; створення цілісної системи захисту інформації. Однак ця модель системи захисту інформації не враховує можливостей здійснення загроз для системи і шляхів захисту від них. Тому, в модель введемо ще два елементи: 1) набір вразливостей $\mathrm{V} = \{v_r\}$, що визначає можливість здійснення загрози T щодо об'єкту захисту O $(\{\mathrm{T}, \mathrm{O}\} : v_r =< t_i, o_j >)$; 2) набір бар'єрів B=$\{\mathrm{b}_l\}$, що визначає шлях здійснення загрози T, перекритий механізмом захисту M $(\{\mathrm{V}, \mathrm{M}\} : b_1 =< t_i, o_j, m_k >)$.

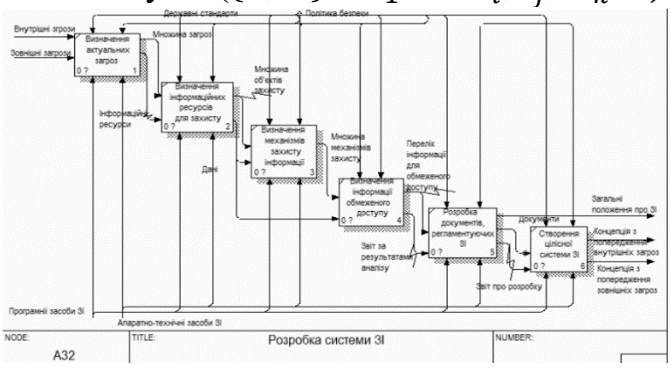

Рисунок 3. Діаграма IDEF0 «Розробка системи захисту інформації» (AS-IS)

Таким чином, враховуючи вищенаведене та [2], систему захисту інформації представимо моделлю, що складається з п'яти елементів: $\{\mathrm{T}, \mathrm{O}, \mathrm{M}, \mathrm{V}, \mathrm{B}\}$. Також необхідно враховувати, що реальна система захисту

інформації може забезпечити лише певний ступінь опірності загрозам безпеки. Тому, кожен елемент множини бар'єрів b_1 поставимо у відповідний набір:

$$< P_1, L_1, R_1 >,$$

де P_1 – ймовірність появи загрози; L_1 – величина збитку при вдалому здійсненні загрози щодо об'єктів захисту; R_1 – ступінь опірності механізму захисту m_k, що характеризується ймовірністю його подолання.

Для оцінки проєктованої системи використаємо ще величину захищеності S, яка згідно з [1] розраховується за формулою:

$$S = 1/Risk_0, \qquad (3.6)$$

де $Risk_0$ – сума всіх залишкових ризиків ($0 < [\mathrm{P_k}, \mathrm{L}_k] < 1;\ 0 < [\mathrm{R}_k] < 1$).

Залишкові ризики характеризують надійність кожного бар'єра і пов'язані з можливістю виконання загрози t_i щодо об'єкта захисту o_j при використанні механізму захисту m_k: $Risk_1 = P_k L_k (1 - R_k)$. Таким чином, враховуючи наведену математичну модель, сформуємо наступні заходи з реінжинірингу процесів системи захисту інформації, а саме процесу «Розробка системи захисту інформації». Запропоновані заходи з реінжинірингу системи відображено на діаграмі IDEF0 «Розробка системи захисту інформації» – рис. 4.

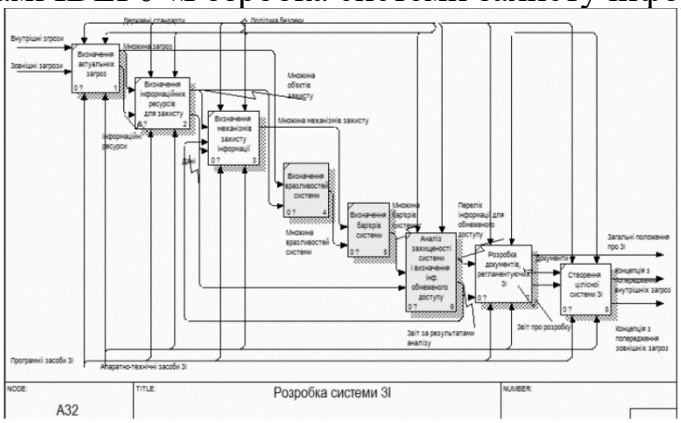

Рисунок 4. Діаграма IDEF0 «Розробка системи захисту інформації»

Таким чином, на основі використання теорії графів, а саме комбінації моделі системи захисту із повним перекриттям та ризик-орієнтованої моделі, було побудовано модель системи захисту інформації.

Література

1. Попова М.С. Применение теории графов при выявлении потенциальных угроз безопасности информации. Проблемы современной науки и образования. 2016. № 35 (77).

2. Черемных С.В. Структурный анализ систем. IDEF-технологии. Финансы и статистика, 2003. 208 с.

3. Рогоза М.Є., Кузьменко О.К., Кропивка О.Г. Інформаційна безпека підприємства: сутність, технологія забезпечення, методи оцінки та моделі. Соціально-економічний розвиток України: моделі, механізми, стратегії: монографія/ за наук. ред. М. Є. Рогози. Полтава : ПУЕТ, 2021. С. 125–146.