УДК 004.056:654.026

В.М. Сидоренко, к.т.н., А.А. Положенцев,
О.Ю. Юдін, к.т.н., О.К. Жигаревич
(Національний авіаційний університет, Україна)

Функціональна модель визначення критичності галузевих інформаційно-телекомунікаційних систем

У даній роботі була розроблена модель, яка дозволяє визначати критичність галузевих ІТС. Представлена модель використовує структурно-логічну та функціональну моделі для визначення функціонального профілю захищеності галузевих ІТС та розрахунку кількісного критерію оцінки захищеності ІТС. Використання цієї моделі дозволить збільшити точність визначення категорії критичності ІТС. Для перевірки адекватності моделі було проведено експериментальне дослідження на прикладі ІТС Національної системи конфіденційного зв'язку (НСКЗ), яке підтвердило правильність реакції моделі на зміну вхідних даних.

Актуальність теми

Завдяки зростаючій кількості та складності кібератак по всьому світу, стало значно складніше захищати інформаційно-телекомунікаційні системи (ІТС), які є критично важливими для ефективної роботи суспільства, економічного зростання країни та забезпечення національної безпеки. У зв'язку з цим, національна безпека та необхідність використання системного підходу до захисту критичної інфраструктури стали пріоритетами при реформуванні сектору оборони та безпеки в Україні. Створення системи захисту такої інфраструктури на загальнодержавному рівні є одним з найважливіших завдань [1].

Законом України «Про основні засади забезпечення кібербезпеки України» [2] передбачено формування переліку об'єктів критичної інфраструктури (ОКІ) та встановлено необхідність розробки порядку віднесення об'єктів до ОКІ. В свою чергу, Постанова КМУ №1109, що стосується ОКІ, містить відомості про Порядок віднесення об'єктів до ОКІ, Перелік секторів (підсекторів) та основних послуг критичної інфраструктури держави та Методику категоризації ОКІ [3], яка визначає механізм віднесення ОКІ до певної категорії критичності на основі аналізу рівня можливого негативного впливу. Крім того, було прийнято Закон України Про критичну інфраструктуру [4], який докладно описує правові та організаційні засади захисту ОКІ при створенні та функціонуванні національної системи захисту критичної інфраструктури.

Тобто, законодавчими актами України задекларовано необхідність розробки нових методів та моделей визначення та оцінювання рівня критичності галузевих ІТС. Використання якісних оцінок для визначення критичності галузевих інформаційно-технологічних систем пов'язане зі складністю порівняння та відтворення таких оцінок. Це пов'язано з викликами підбору експертів та обробки експертних даних. Як наслідок, існує наукове завдання створення функціональної моделі для визначення та розрахунку критичності галузевих інформаційно-технологічних систем.

Опис моделі визначення критичності галузевих ІТС

Розроблена модель визначення критичності галузевих ІТС відрізняється від відомих методів [5-6], оскільки вона базується на властивостях інформації, таких як конфіденційність, цілісність, доступність та спостереженість, а також враховує кількісні показники критеріїв віднесення до критичної інфраструктури [1, 6-7]. На рис. 1 показана блок-схема реалізації моделі, яка використовує результати структурно-логічної моделі формування функціонального профілю захищеності галузевої ІТС, структурно-функціонального методу формування ФПЗ галузевої ІТС та моделі розрахунку кількісного критерію оцінки захищеності ІТС.

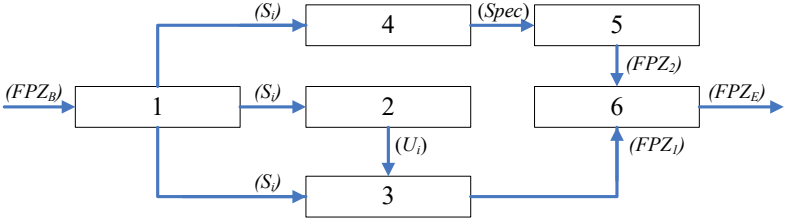

Рис.1. Реалізація функціональної моделі визначення критичності галузевих ІТС

Спершу, у блоці 1 визначаються підсистем ІТС та її компоненти ($S_1, S_2, ...S_n, S_{i1}, S_{i2}, ...S_{im}, S_{ij1}, S_{ij2}, ...S_{ijr_{ij}}, C_1, C_2, ...C_b$).

Блок 2 відповідає за визначення функцій кожного виявленого компонента системи, формує перелік можливих порушень роботи кожного компонента системи, оцінює наслідки кожного з можливих порушень роботи ($F_1, F_2, ...F_l, D_1, D_2, ...D_p, E_1, E_2, ...E_q$).

Блок 3 відповідає за визначення рівня критичності можливих порушень для кожного наслідку порушення та кожного компонента підсистеми ($R_{E_i}, R_{D_i}, R_{C_{ijkl}}$).

Блок 4 відповідає за обчислення рангів критичності ймовірних порушень підсистем ($\overline{R_{S_{ij}}}$).

Результати експериментального дослідження

У роботі [1] була перевірена експериментальна модель визначення критичності галузевих ІТС, використовуючи структурно-функціональний метод визначення ФПЗ галузевої ІТС. Було отримано базовий та відкоригований ФПЗ Національної системи конфіденційного зв'язку (НСКЗ) на основі запропонованого методу:

- FPZB: КА-2, КВ-3, КД-2, КО-1, ЦА-2, ЦВ-2, ЦД-1, ЦО-2, ДС-2, ДЗ-2, ДВ-2, ДР-2, НА-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НР-2, НВ-2, НП-1;
- FPZE: КА-3, КВ-4, КД-3, КО-1, КК-2, ЦА-4, ЦВ-2, ЦД-1, ЦО-2, ДС-2, ДЗ-2, ДВ-3, ДР-3, НА-1, НИ-2, НК-1, НО-3, НЦ-3, НТ-3, НР-5, НВ-2, НП-1.

FPZE є важливим елементом в оцінці рівня захищеності НСКЗ та визначенні критичності її роботи та визначається як критерій оцінки захищеності інформації, що в ній оброблюється.

Використовуючи метод розрахунку кількісного критерію оцінки захищеності НСКЗ за допомогою методу аналізу ієрархій отримуємо значення $VK_{AHP} = 0,717$, що зображено на рис. 2.

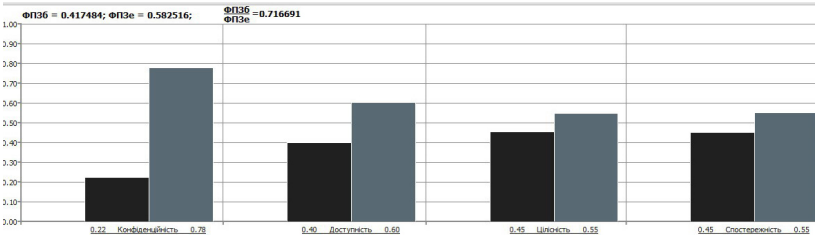

Рис. 2. Результати обчислень відношення між альтернативами

Крім того, у роботі було виконано розподілення НСКЗ на класи систем S_i, множини систем класів S_{ij}, та їх складових підсистем S_{ijk}, відповідно до табл. 4 [8]). Також були описані складові системи C_{ijkl}, що є в основі всіх підсистем S_{ijk}.

Також, виконана декомпозиція НСКЗ на класи систем S_i, множини систем що входять до класів S_{ij}, та їх підсистеми S_{ijk} (згідно табл. 4 в роботі [8]), а також визначені компоненти C_{ijkl}, з яких складається кожна підсистема S_{ijk}. Для кожного компонента підсистеми визначено список можливих функцій F_i, порушень D_i, наслідків E_i та рангів критичності *REi*. Застосувавши модель визначення критичності галузевих ІТС, було розраховано ранги критичності R_{D_i} для порушень роботи компонента D_i у підсистемі C_{ijkl}, ранги критичності ймовірних порушень $R_{C_{ijkl}}$ для компонента C_{ijkl}, ранги критичності ймовірних порушень $\overline{R_{S_{ijk}}}$ та $\overline{R_{S_{ij}}}$ для підсистем S_{ijk} і S_{ij}, ранги критичності ймовірних порушень R_{S_i} для систем S_i, а також загальний ранг критичності R_S НСКЗ (*S*).

Зазначимо, що з урахуванням отриманих у роботі [8] даних, був розрахований коефіцієнт тяжкості наслідків від порушення функціонування НСКЗ, який дорівнює $VK = 0,37$. Середнє арифметичне зважене рангу порушення для НСКЗ, складає $\overline{R_S} = 51,40$. На підставі розрахунків було отримано числове значення рангу критичності, яке складає $R_S = 190,7$. З цього можна зробити висновок, що на даний момент НСКЗ не вважається критичною галузевою ІТС.

Висновки

Отже, у цій роботі пропонується вдосконалена модель для визначення критичності галузевих ІТС, яка базується на використанні структурно-логічної моделі та структурно-функціонального методу формування ФПЗ галузевої ІТС, а також моделі розрахунку кількісного критерію оцінки захищеності ІТС з використанням методу аналізу ієрархій. Використання цієї моделі дозволяє приймати рішення щодо віднесення ІТС до категорії критичних, з урахуванням властивостей інформації, таких як конфіденційність, цілісність, доступність та спостереженість.

Також було проведено експериментальне дослідження розробленої моделі, За допомогою якої було розраховано ранги критичності порушень роботи компонентів, підсистем та систем НСКЗ, кількісний показник коефіцієнта тяжкості наслідків від порушень функціонування НСКЗ, а також кількісний показник рангу критичності НСКЗ. На основі цих розрахунків зроблено висновок щодо критичності.

Список літератури

1. С.О. Гнатюк, В.М. Сидоренко, О.Ю. Юдін, Т.В. Смірнова, С.Ю. Сидоренко «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем» Проблеми інформатизації та управління. – 2022. – Т. 2. – № 70. – С. 28-37.
2. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2021) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Постанова Кабінету Міністрів України № 1109 (2020) (Україна). https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#n45
4. Про критичну інфраструктуру, Закон України № 1882-IX (2021) (Україна). https://zakon.rada.gov.ua/laws/show/1882-20#Text
5. Gritzalis D., Theocharidou M., Stergiopoulos G., Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies, Springer, 2019, 311 p. (Advanced Sciences and Technologies for Security Applications). ISBN 978-3-030-00023-3.
6. Л.М. Щербак, С.О. Гнатюк, В.М. Сидоренко, О.А. Шаховал, Метод визначення рівня важливості об’єктів критичної інформаційної інфраструктури в галузі цивільної авіації, Безпека інформації, Том 23, №1, 2017.
7. С.О. Гнатюк, О.Ю. Юдін, В.М. Сидоренко, Я.П. Євченко «Метод формування функціонального профілю захищеності галузевих інформаційно-телекомунікаційних систем», Кібербезпека: освіта, наука, техніка, 2021, Т. 3, № 11, С. 166-182.
8. Гнатюк С. О., Сидоренко В. М., Юдін О. Ю., Смірнова Т. В., «Метод розрахунку критичності галузевих інформаційно-телекомунікаційних систем», Наукоємні технології, Вип. №2(54), С. 94-104, 2022.