УДК 004.056:654.026

DOI: 10.18372/2073-4751.70.16844

Гнатюк С.О., д.т.н.,
orcid.org/0000-0003-4992-0564,
Сидоренко В.М., к.т.н.,
orcid.org/0000-0002-5910-0837,
Юдін О.Ю., к.т.н.,
orcid.org/0000-0002-4730-1463,
Смірнова Т.В., к.т.н.,
orcid.org/0000-0001-6896-0612,
Сидоренко С.Ю.

МОДЕЛЬ ВИЗНАЧЕННЯ КРИТИЧНОСТІ ГАЛУЗЕВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Національний авіаційний університет
Центральноукраїнський національний технічний університет

s.gnatyuk@nau.edu.ua

Вступ

Світові тенденції до збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту інформаційно-телекомунікаційних систем (ІТС), зокрема, галузевих, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення інформаційної складової національної безпеки. З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми захисту критичної інфраструктури, на загальнодержавному рівні, створення системи захисту такої інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України [1].

Необхідно зазначити, що Законом України «Про основні засади забезпечення кібербезпеки України» [2] визначено необхідність формування переліку об'єктів критичної інфраструктури (ОКІ) та необхідність розробки порядку віднесення об'єктів до ОКІ. Постанова КМУ №1109, про деякі питання ОКІ затверджує: Порядок віднесення об'єктів до ОКІ; Перелік секторів (підсекторів) та основних послуг критичної інфраструктури держави; та Методику категоризації ОКІ [3]. Зазначена Методика описує механізм віднесення ОКІ до певної категорії критичності, який визначається на основі аналізу рівня можливого негативного впливу. Крім того, нещодавно, набув чинності Закон України Про критичну інфраструктуру [4], який детально описує правові та організаційні засади захисту ОКІ під час створення та функціювання національної системи захисту критичної інфраструктури.

Таким чином, нормативно-правовими актами України задекларовано необхідність розробки нових методів та моделей визначення та оцінювання рівня критичності галузевих ІТС. При цьому доцільно зазначити, що використання якісних оцінок пов'язане зі складністю їх порівнювання та відтворювання. Насамперед, це обумовлено складністю підбору експертів і специфікою обробки експертних даних. Зазначені обмеження свідчать про наявність важливого наукового завдання щодо визначення та розрахунку критичності галузевих ІТС.

Мета

Мета статті – провести аналіз існуючих моделей визначення і розрахунку критичності ІТС; на основі результатів аналізу розробити функціональну модель визначення критичності галузевих ІТС.

Аналіз останніх досліджень та публікацій

Шведська модель визначення критичності ОКІ, що заснована на національній оцінці ризику (Swedish National Risk

Assessment 2012) [5], представлена на рис. 1.

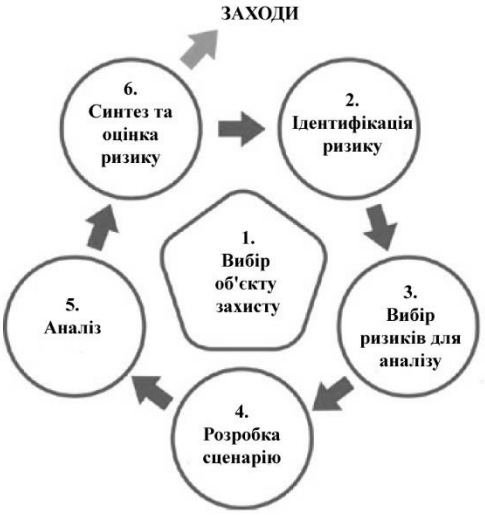

Рис. 1. Шведська модель визначення ОКІ

На першому етапі здійснюється вибір об'єкту захисту. При виборі об'єктів захисту враховуються шкода, яка може бути заподіяна: здоров'ю громадян, повсякденному життю громадян, органам управління державою, економічним активам держави, навколишньому середовищу, суверенітету держави.

На другому етапі здійснюється ідентифікація ризиків виникнення події. Ідентифікація ризиків виявляє перелік подій які гіпотетично можуть загрожувати об'єктам захисту. При цьому формується опис вартості захисту, загрози та шляхи виникнення загрози. На підставі цього формується базовий каталог. Другий етап не ідентифікує остаточно події як ризики.

На третьому етапі здійснюється вибір подій для аналізу. Ідентифіковані на другому етапі ризики настання подій оцінюються за ймовірністю та тяжкістю наслідків. З деякою періодичністю ризики та події переглядаються.

На четвертому етапі здійснюється розробка сценарію який описує хід подій при реалізації ризику. При створенні сценарію враховується велика ймовірність його виникнення.

На п'ятому етапі здійснюється аналіз сценарію. Аналіз здійснюється з урахуванням ймовірності його виникнення та тяжкості наслідків. Наслідки розвитку сценарію оцінюються на основі п'яти категорій: функціонування суспільства; життя та здоров'я людини; економіка та навколишнє середовище; демократія, верховенство права, права та свободи людини; національний суверенітет.

На шостому етапі здійснюється синтез та оцінка ризику. Метою цього етапу є здійснення висновків за п'ятим етапом. Результати зводяться в матрицю ризиків (рис. 2).

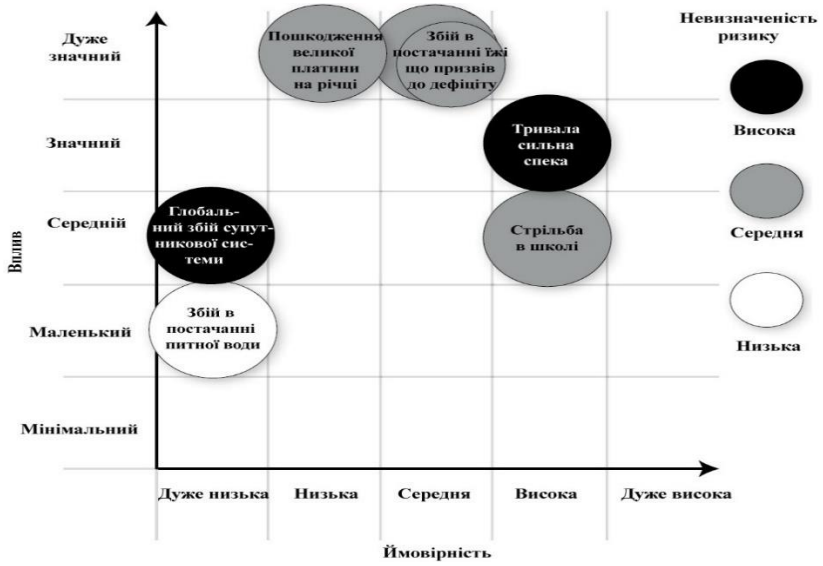

Рис. 2. Шведська модель матриці ризиків

Останній етап це вибір заходів протидії. На останньому етапі визначаються пріоритети щодо захисту, заходи стосовно забезпечення захисту та попередження.

Німецька модель визначення критичності ОКІ [6] має наступний вигляд (рис. 3).

Рис. 3. Німецька модель визначення ОКІ

Перший етап містить в собі розподіл на сектори критичної інфраструктури та здійснення опису цих секторів. При цьому, сектори описуються для кожної галузі. Наприклад: транспортний сектор має складові – наземна, авіаційна, морська. Кожна з цих складових описується окремо.

Другим етапом є ідентифікація бізнес–процесів. Ідентифікація, як правило, здійснюється експертами. Приклад бізнес-процесу – постачання нафти (енергетичний сектор), яке складається з чотирьох етапів: видобуток, переробка, транспортування, постачання користувачу. На кожному етапі ідентифікуються процеси та ризики.

Третій етап це оцінка критичності. На цьому етапі ключовою є відповідь на питання «Що станеться, якщо один з компонентів в процесі роботи вийде із ладу і яка ймовірність цього». Оцінка критичності здійснюється експертами без числових показників, натомість використовуються поняття «звичайний», «низький», «помірний», «величезний», «катастрофічний». Таким чином отримують критичність процесу виходячи з комбінації ймовірності та можливого ефекту.

Після здійснення оцінки критичності окремі процеси вводяться в матрицю критичності (рис. 4). Критичність всіх процесів оцінюється крізь призму рівнів абстракцій «Бізнес», «Сектор», «Суспільство». Процеси, чиї признаки критичності визнаються «низькими» або «середніми» можуть бути проігноровані. Для наступної обробки є обов'язковими процеси з признаками «Значущий» і «Високий».

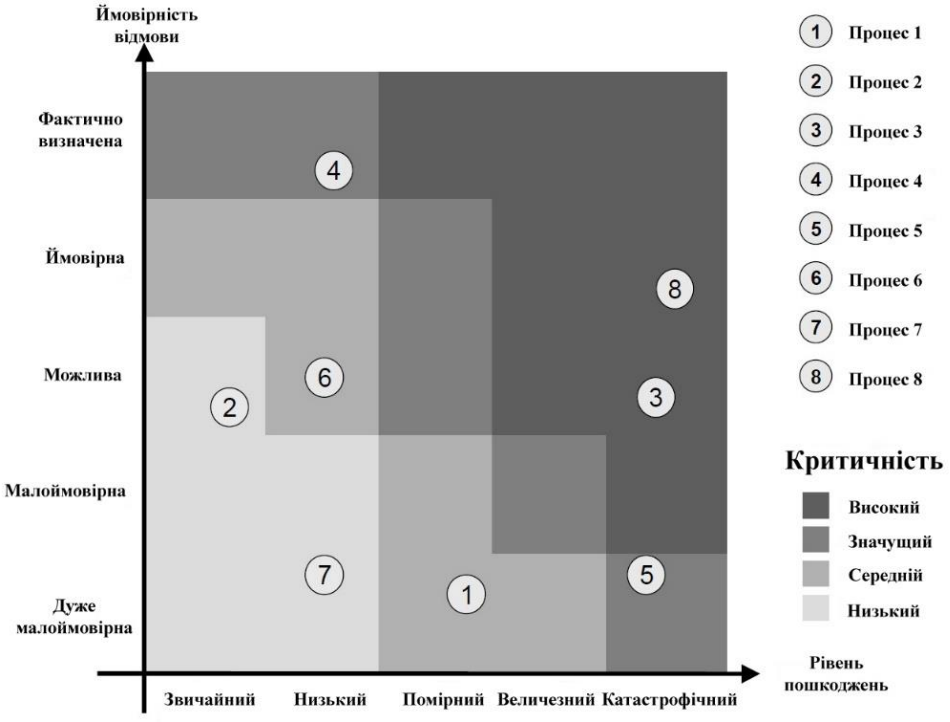

Рис. 4. Матриця критичних процесів

Четвертим етапом є дослідження залежностей між процесами і секторами. Загальна схема процедури віднесення до критичної інфраструктури, з урахуванням залежності, зображена на рис. 5.

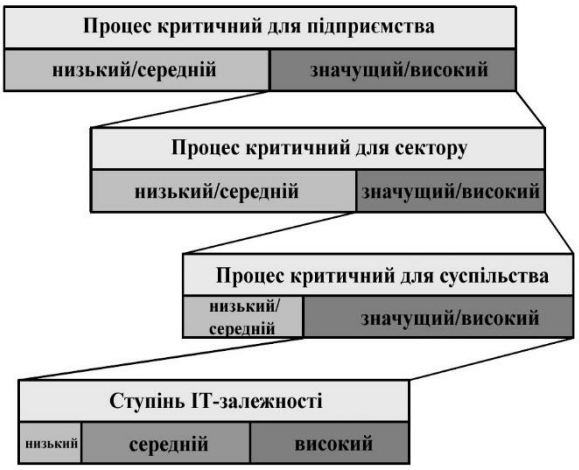

Рис. 5. Спрощена процедура віднесення до критичної інфраструктури

П'ятим етапом є коригування. Під час коригування застосовуються поправочні коефіцієнти. До цих коефіцієнтів можуть відноситись: вже реалізовані механізми захисту, кваліфікація експертів які здійснювали оцінку.

Останнім етапом є визначення критичності на базі звітів. До звітів входять відомості щодо аналізу критично-важливої інфраструктури сектору (дані щодо ступеню важливості, загального опису важливих бізнес-процесів, матриці критичних процесів, залежності процесів та секторів).

Модель визначення та захисту ОКІ США [7] представляє собою модель постійного удосконалення захисту критичної інфраструктури та ключових ресурсів (КІКР) (рис. 6):

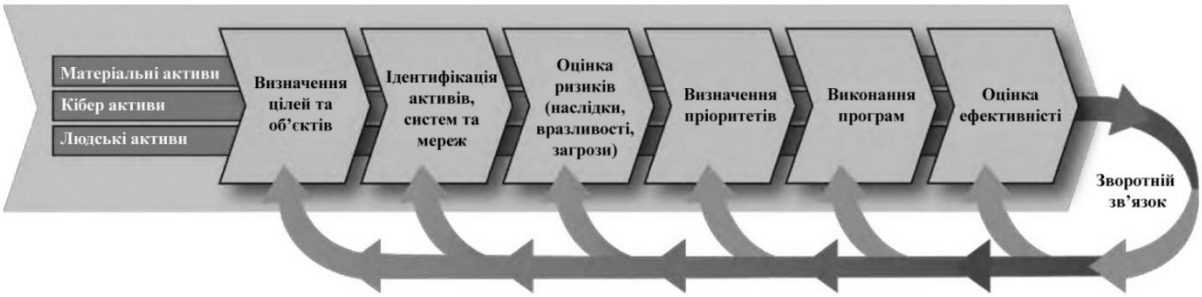

Рис. 6. Модель визначення та захисту ОКІ США

Визначення цілей та об'єктів здійснюється з урахуванням фізичних ресурсів, кібер ресурсів, захисту населення та відмовостійкості критичних систем. За базу для визначення цілей беруться вже існуючи профілі ризику різних секторів та географічних регіонів.

Також, під час визначення об'єктів, здійснюється аналіз власника об'єкту (національний, регіональний, галузевий і таке інше).

Ідентифікацією активів, систем та мереж займається Департамент внутрішньої безпеки США (DHS). DHS виконує постійну інвентаризацію активів що складають КІКР США та формує відповідний національний кадастр (IDW – Infrastructure Data Warehouse). До IDW входять відомості щодо стихійних лих, промислових аварій та інших інцидентів, а також щодо взаємозв'язків активів.

Оцінка ризиків (наслідки, вразливості, загрози) здійснюється за чотирма категоріями:

- охорона здоров'я та безпека;
- економічні втрати (прямі та опосередковані);
- психологічний стан населення;
- управління державою.

При оцінці ризику розглядаються всі 18 секторів КІКР. Основними критеріями для оцінки ризиків є:

- документування інформації та механізмів її синтезу;
- використання відтворюваних результатів;
- ймовірність ризику повинна бути доказана;

• оцінка повинна надавати конкретні рекомендації для кожного сценарію.

За результатами оцінки ризиків формуються переліки можливих наслідків.

Визначення пріоритетів дозволяє спрямувати зусилля по керуванню ризиками в найбільш значимий КІКР.

Виконання програм захисту та забезпечення відмовостійкості полягає у структуризації необхідних дій для захисту КІКР. Деякі програми фінансуються державою, деякі операторами систем на базі різноманітних стимулів. Програми координують зусилля та найбільш економічно ефективно розподіляють ресурс.

Оцінка ефективності виконується на базі різних показників. Під час оцінки відслідковується прогрес в досягненні цілі шляхом об'єктивно виміряних даних щодо підвищення захищеності національних та галузевих КІКР. За збір даних відповідає DHS.

Зворотній зв'язок забезпечує розуміння того, які галузі потребують додаткової уваги (фінансування, регулювання)

З урахуванням зазначеного вбачається за доцільне враховувати критичність галузі, функціонування якої вона забезпечує та розробити власну функціональну модель визначення критичності галузевих ІТС.

Модель визначення критичності галузевих ІТС

Модель визначення критичності галузевих ІТС, на відміну від відомих моделей та методів [8-13], базується на використанні таких властивостей інформації, як конфіденційність, цілісність, доступність, спостереженість, а також враховує кількісні показники критеріїв віднесення до критичної інфраструктури [14-15].

В загальному випадку модель можна представити у вигляді блок-схеми (рис. 7). Запропонована модель використовує результати структурно-логічної моделі формування функціонального профілю захищеності галузевої ІТС, структурно-функціонального методу формування ФПЗ галузевої ІТС, а також моделі розрахунку кількісного критерію оцінки захищеності ІТС.

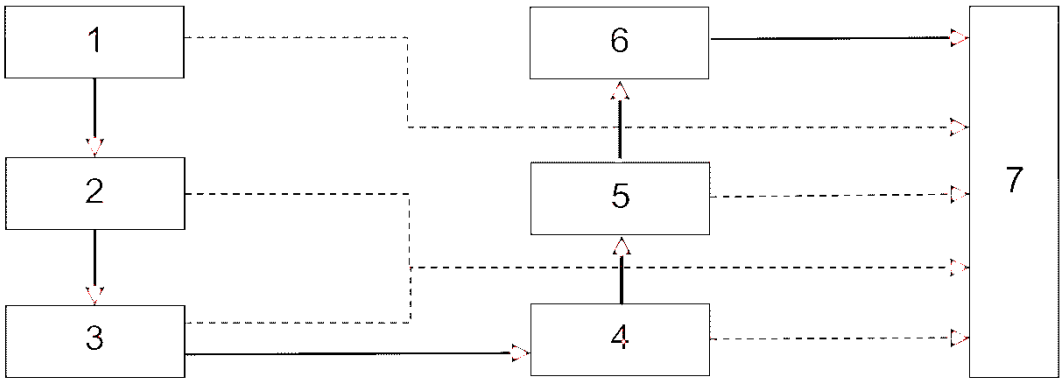

Рис. 7. Блок-схема реалізації функціональної моделі визначення критичності галузевих ІТС

У блоці 1 здійснюється визначення підсистем ІТС та її компонентів ($S_1, S_2, ...S_n, S_{i1}, S_{i2}, ...S_{im}, S_{ij1}, S_{ij2}, ...S_{ijr_{ij}}, C_1, C_2, ...C_b$).

У блоці 2 визначаються функції кожного виявленого компонента системи, формується перелік можливих порушень роботи кожного компонента системи, оцінюються наслідки кожного з можливих порушень роботи:
($F_1, F_2, ...F_l, D_1, D_2, ...D_p, E_1, E_2, ...E_q$).

В блоці 3 визначаються ранги критичності ймовірних порушень для кожного наслідку порушень та кожного порушення компонента підсистеми ($R_{E_i}, R_{D_i}, R_{C_{ijkl}}$).

В блоці 4 відбувається обчислення рангів критичності ймовірних порушень підсистем ($\overline{R_{S_{ij}}}$)

У блоці 5 здійснюється розрахунок рангів критичності ймовірних порушень систем та ІТС в цілому(R_S)

У блоці 6 відбувається віднесення ІТС до категорії критичних або некритичних

У блоці 7 формується загальний звіт.

Зазначена модель дозволяє здійснити прийняття рішення про віднесення ІТС до категорії критичних з урахуванням властивостей інформації, як конфіденційність, цілісність, доступність, спостереженість.

Експериментальна перевірка моделі визначення критичності галузевих ІТС

На основі запропонованого у роботі [1] структурно-функціонального методу визначення ФПЗ галузевої ІТС отримано базовий та відкоригований ФПЗ Національної системи конфіденційного зв'язку (НСКЗ):

- 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 критерієм оцінки захищеності інформації, що циркулює в НСКЗ.

За допомогою методу розрахунку кількісного критерію оцінки захищеності НСКЗ з використанням методу аналізу ієрархій отримане значення $VK_{AHP} = 0{,}717$. Результат розрахунку VK_{AHP} наведений на рис. 8.

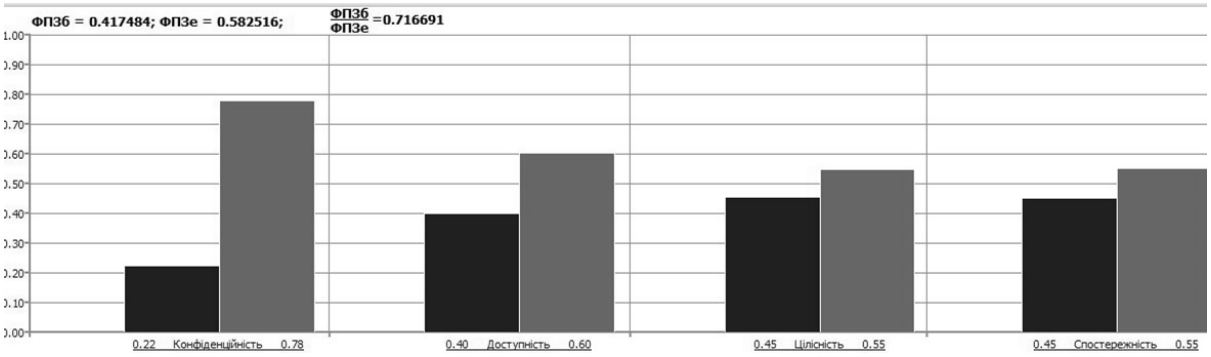

Рис. 8. Результат розрахунків співвідношення альтернатив

Також, виконана декомпозиція НСКЗ на класи систем S_i, множини систем що входять до класів S_{ij}, та їх підсистеми S_{ijk} (табл.1 в роботі [1] та табл.4 в роботі [16], а також визначені компоненти C_{ijkl}, з яких складається кожна підсистема S_{ijk}. Фрагмент декомпозиції наведений в табл. 1.

Таблиця 1. Декомпозиція НСКЗ на компоненти

Рівень	Кількість елементів	Позначення системи/підсистеми/компоненту
1	4	S_t, S_s, S_d, S_m
2	10	S_{t1}, S_{t2}, S_{t3}, S_{s1}, S_{s2}, S_{d1}, S_{d2}, S_{d3}, S_{m1}, S_{m2}
3	34	S_{t11}, S_{t12}, S_{t13}, ….., S_{m23}, S_{m24}
4	115	C_{t111}, C_{t112}, C_{t113}, ….., C_{m231}, C_{m241}

Для кожного з компонентів підсистеми визначений перелік функцій F_i, можливих порушень функціонування D_i, наслідків E_i та рангів критичності наслідків REi. Фрагмент переліку наведений в табл. 2.

Використовуючи модель визначення критичності галузевих ІТС, здійснений розрахунок рангів критичності R_{D_i}порушення роботи D_iкомпонента C_{ijkl}, рангів критичності ймовірних порушень $R_{C_{ijkl}}$ компонент C_{ijkl} підсистеми, рангів критичності ймовірних порушень $\overline{R_{S_{ijk}}}$ та $\overline{R_{S_{ij}}}$підсистем S_{ijk} і S_{ij}, рангів критичності ймовірних порушень R_{S_i}систем S_i та в цілому R_S НСКЗ (S). Фрагмент результатів розрахунку наведений в табл. 3.

Таблиця 2. Перелік функцій, можливих порушень, наслідків та рангів критичності

Ci	*Cijkl*	*ФПЗ*	*Fi*		*Di*		*Ei*		*Rei*	*B1i*	*B2i*	*B3i*
C_{t11}	Телефон	ДС-1, ДВ-1, НТ-2	F_{t1111}	Формування електричного сигналу	D_{t11111}	Відсутність електроживлення	$E_{t111111}$	Відсутність зв'язку	1	1,0	1,0	1,0
							$E_{t111112}$	Неможливість протокол. роботи	5	1,0	5,0	1,0
			F_{t1112}	Аналіз та формування мережевого пакету (ARP, Ethernet, IP…)	D_{t11121}	Пошкодження апаратного забезпечення	$E_{t111211}$	Відсутність зв'язку	1	1,0	1,0	1,0
					D_{t11123}	Некоректні налаштування	$E_{t111231}$	Відсутність зв'язку	2	2,0	1,0	1,0

Таблиця 3. Результати розрахунку рангів критичності

Sijk	*Ci*	*Fi*	*Di*	*Ei*	*Rei*	*Rdijk*	*Rcij*	*Rsijk*	*Rsij*	*Rsi*	*Rs*
S_{t11}	C_{t111}	F_{t1111}	D_{t11111}	$E_{t111111}$	1	3,00	1,87	6,34	13,00	29,95	51,40
				$E_{t111112}$	5						
			D_{t11112}	$E_{t111121}$	1	1,00					
			D_{t11113}	$E_{t111131}$	1	2,33					
				$E_{t111132}$	5						
				$E_{t111133}$	1						
		F_{t1112}	D_{t11121}	$E_{t111211}$	1	1,00					
			D_{t11123}	$E_{t111231}$	2	2,00					
	C_{t113}	F_{t1131}	D_{t11311}	$E_{t113111}$	2	2,00	1,75				
				$E_{t113112}$	2						
			D_{t11312}	$E_{t113121}$	2	1,50					
				$E_{t113122}$	1						
…	…	…	…	…	…	…	…	…	…	…	
S_{m24}	C_{m241}	F_{m2411}	D_{m24113}	E_{m24113}	50	2,00	40	40	40	25,78	

З урахуванням даних наведених в табл. 7 в роботі [16] зроблений розрахунок коефіцієнту тяжкості наслідків від порушення функціонування НСКЗ $VK = 0{,}37$.

Середнє арифметичне зважене рангу порушення для НСКЗ, складає $\overline{R_S} = 51{,}40$.

За результатами розрахунку отриманий кількісний показник рангу критичності, який дорівнює $R_S = 190{,}7$, та зроблений висновок, що НСКЗ, на теперішній час, не відноситься до критичних ІТС.

Висновки

У роботі було проведено аналіз моделей визначення критичності галузевих ІТС, який показав, що: найчастіше визначення рівня критичності відбувається через оцінку ризиків, що не відповідає вимогам НД ТЗІ; методи оцінки ризику, які аналізують наслідки, ймовірність настання та рівень ризику, не здійснюють ідентифікацію відмов за властивостями інформації (КЦДС); доцільно враховувати критичність певної галузі

Також в роботі представлено удосконалену модель визначення критичності галузевих галузевих ІТС, яка використовує результати структурно-логічної моделі та структурно-функціонального методу формування ФПЗ галузевої ІТС, а також моделі розрахунку кількісного критерію оцінки захищеності ІТС яка базується на використанні методу аналізу ієрархій. Використання розробленої моделі дозволяє здійснити прийняття рішення про віднесення ІТС до категорії критичних з урахуванням властивостей інформації, як конфіденційність, цілісність, доступність, спостереженість.

Крім того, у статті представлено експериментальне дослідження запропоно-

ваної моделі. Використовуючи дану модель, здійснено розрахунок рангів критичності порушення роботи компонент, підсистем та систем НСКЗ, розрахунок кількісного показника коефіцієнту тяжкості наслідків від порушення функціонування НСКЗ, а також розраховано кількісний показник рангу критичності НСКЗ та, на підставі цього, зроблений висновок щодо критичності НСКЗ.

Література

1. *Гнатюк С.О., Юдін О.Ю., Сидоренко В.М., Євченко Я.П.*. Метод формування функціонального профілю захищеності галузевих інформаційно-телекомунікаційних систем. Кібербезпека: освіта, наука, техніка. – Т. 3. – № 11. – 2021. – С. 166-182.

2. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2021) (Україна). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Постанова Кабінету Міністрів України № 1109 (2020) (Україна). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#n45

4. Про критичну інфраструктуру, Закон України № 1882-IX (2021) (Україна). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text

5. Swedish National Risk Assessment 2012. Swedish Civil Contingencies Agency. Order No: MSB556. June 2013. ISBN: 978-91-7383-339-4. [Електронний ресурс]. – Режим доступу: https://www.msb.se /RibData/Filer/pdf/26621.pdf. – Назва з екрану.

6. Bundesamt für Sicherheit in der Informationstechnik. Analysis of Critical Infrastructures - The ACIS methodology - (Analysis of Critical Infrastructural Sectors). BSI KRITIS, 4/2004. [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de /SharedDocs/Downloads/EN/BSI/Kritis/acis _paper_en_pdf.pdf?__blob=publicationFile.

7. National Infrastructure Protection Plan. Partnering to enhance protection and resiliency. 2009. Homeland Security. [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

8. *Щербак Л.М., Гнатюк С.О., Сидоренко В.М., Шаховал О.А.* Метод визначення рівня важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації. Безпека інформації. – Том 23. – №1. – 2017. – С. 27-38.

9. *Сидоренко В.М, Гнатюк С.О, Юдін О.Ю.* Експериментальне дослідження методу визначення рівня важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації. Захист інформації. – Т. 19. – № 2. – 2017. С. 155-172.

10. *Sydorenko V., Gnatyuk S., Tolbatov A., Fesenko A., Yevchenko Ya., Sotnichenko Yu.* Experimental FMECA-based Assessing of the Critical Information Infrastructure Importance in Aviation», CEUR Workshop Proceedings. Proceedings of the 16th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer (ICTERI 2020), October 06-10, 2020. – Vol. 2732. – P. 136-156.

11. *Gnatyuk S., Sydorenko V., Polihenko O., Sotnichenko Yu., Nechyporuk O.* Studies on the Disasters Criticality Assessment in Aviation Information Infrastructure. CEUR Workshop Proceedings. Proceedings of the 1st International Workshop on Computational & Information Technologies for Risk-Informed Systems (CITRisk 2020), October 15-16, 2020. – Vol. 2805. – P. 282-296.

12. *Stergiopoulos G., Kouktzoglou V., Theocharidou M., Gritzalis D.* A process-based dependency risk analysis methodology for Critical Infrastructures // Int. J. Critical Infrastructures. – Vol. 13. – №. 2/3. – 2017. – P. 184-205.

13. *Gritzalis D., Theocharidou M., Stergiopoulos G.,* Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies. Advanced Sciences and Technologies for Security Applications. – Springer, 2019. – 311 p.

14. *Юдін О.* Метод визначення критичності галузевих інформаційно-телекомунікаційних систем. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 1(35). – 2018. – С. 80-91.

15. Звіт про НДР «Дослідження та аналіз проблем захисту інформації на об'єктах критичної інфраструктури», шифр «Інфрастуктура» (д.р. №0114U000038д).

16. *Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Смірнова Т.В.* Метод розрахунку критичності галузевих інформаційно-телекомунікаційних систем. Наукоємні технології. – Вип. № 2(54). – 2022. – С. 94-104.

Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Смірнова Т.В., Сидоренко С.Ю.

МОДЕЛЬ ВИЗНАЧЕННЯ КРИТИЧНОСТІ ГАЛУЗЕВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Світові тенденції до збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту інформаційно-телекомунікаційних систем (ІТС), зокрема, галузевих, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення інформаційної складової національної безпеки. З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми захисту критичної інфраструктури, на загальнодержавному рівні, створення системи захисту такої інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України. Таким чином, виникає необхідність розробки методів та моделей віднесення інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури для забезпечення національної безпеки України. У роботі представлено модель визначення критичності галузевих ІТС, що за рахунок використання структурно-логічної та функціональної моделі визначення функціонального профілю захищеності галузевої ІТС, а також функціональної моделі розрахунку кількісного критерію оцінки захищеності ІТС дозволяє підвищити точність прийняття рішення про віднесення ІТС до категорії критичних. Використання розробленої моделі дозволяє здійснити прийняття рішення про віднесення ІТС до категорії критичних з урахуванням властивостей інформації, як конфіденційність, цілісність, доступність, спостереженість. Крім того, було проведено експериментальне дослідження запропонованої моделі на прикладі ІТС Національної системи конфіденційного зв'язку (НСКЗ), за допомогою якого перевірено адекватність реагування моделі на зміну вхідних даних. Використовуючи модель визначення критичності галузевих ІТС здійснений розрахунок рангів критичності порушення роботи компонент, підсистем та систем НСКЗ, розрахунок кількісного показника коефіцієнту тяжкості наслідків від порушення функціонування НСКЗ, а також розрахований кількісний показник рангу критичності НСКЗ та, на підставі цього, зроблений висновок щодо критичності НСКЗ.

Ключові слова: *інформаційно-телекомунікаційні системи (ІТС), критична інфраструктура, об'єкт критичної інфраструктури, критичність, ранг критичності, функціональний профіль захищеності.*

Gnatyuk S.O., Sydorenko V.M., Yudin O.Yu., Smirnova T.V., Sydorenko S.Yu.

MODEL FOR DETERMINING THE CRITICALITY OF SECTORAL INFORMATION AND TELECOMMUNICATION SYSTEMS

Global trends towards an increase in the number and complexity of cyber-attacks led to the actualization of the issue of information and telecommunication systems (ITS) protection. In particular, sectoral ITS, which are critically important for the functioning of society, the socio-economic development of the state and ensuring the informational component of national

security. Taking into account the needs of national security and the need to introduce a system approach to solving the problem of protecting critical infrastructure, at the national level, creating a system for protecting such infrastructure is one of the priorities in the reform of the defense and security sector of Ukraine. Thus, there is a need to develop methods and models for the including of ITS to critical information infrastructure to ensure the national security of Ukraine. The paper presents a model for calculating the level of criticality of sectoral ITS, which, due to the use of a structural-logical and functional model for determining the functional profile of the security of a sectoral ITS, as well as a functional model for calculating the quantitative criterion for assessing the security of ITS, made it possible to increase the accuracy of the decision to assign ITS to the critical category. The use of the developed model makes it possible to make a decision to assign ITS to the category of critical, taking into account the properties of information, such as confidentiality, integrity, availability, observability. In addition, an experimental study of the proposed method was carried out on the example of the ITS of the National Confidential Communication System (NCCS), which verified the adequacy of the method's response to changes in input data. Using the model of calculating the criticality of branch ITs, the calculation of the criticality ranks of malfunctioning of components, subsystems and systems of NCCS was carried out, the calculation of the quantitative indicator of the severity factor of the consequences of the malfunctioning of NCCS, as well as the quantitative indicator of the rank of criticality of NCCS was calculated and, based on this, a conclusion was made regarding the criticality of NCCS.

Keywords: *information and telecommunication systems (ITS), critical infrastructure, critical infrastructure object, criticality, criticality rank, functional security profile.*