© Saliieva O., Yaremchuk Yu. Cognitive model for studying the level of protection of a critical infrastructure object // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 2, pp. 64-73.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

DOI: 10.18372/2225-5036.26.14915

КОГНІТИВНА МОДЕЛЬ ДЛЯ ДОСЛІДЖЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Ольга Салієва, Юрій Яремчук

Вінницький національний технічний університет

САЛІЄВА Ольга Володимирівна

Рік та місце народження: 1982 рік, м. Вінниця, Україна.
Освіта: Вінницький державний педагогічний інститут ім. М. Коцюбинського, 2004 рік; Вінницький національний технічний університет, 2018 рік.
Посада: аспірантка кафедри менеджменту та безпеки інформаційних систем з 2016 року.
Наукові інтереси: нечітка математика, безпека інформаційних систем.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на наукових конференціях, свідоцтва про реєстрацію авторського права на твір.
E-mail: salieva8257@gmail.com.
Orcid ID: 0000-0003-2388-7321.

ЯРЕМЧУК Юрій Євгенович, д.т.н., професор

Рік та місце народження: 1974 рік, м. Вінниця, Україна.
Освіта: Вінницький національний технічний університет, 1996 рік.
Посада: директор Центру інформаційних технологій та захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем, з 2010 року.
Наукові інтереси: криптографічний та стеганографічний захист інформації, технічний захист інформації, безпека інформаційних систем.
Публікації: понад 270 публікацій, у тому числі 2 монографії, 140 статей у наукових фахових виданнях, 20 підручників та навчальних посібників, автор 20-ти патентів на корисну модель та 20-х свідоцтв про реєстрацію авторського права на твір.
E-mail: yurevyar@vntu.edu.ua.
Orcid ID: 0000-0002-6303-7703.

Анотація. *Для вирішення питань щодо забезпечення захищеності об'єктів критичної інфраструктури необхідно проаналізувати потенційні загрози, дослідити взаємозв'язки між ними та визначити вплив даних загроз на досліджувану систему. При цьому з'являються деякі труднощі пов'язані із високим ступенем невизначеності, складністю строгої формалізації та суб'єктивним характером даних задач. У зв'язку з цим у роботі пропонується використання когнітивного підходу, який не потребує великого обсягу експериментальних даних, надає можливість опрацьовувати доступну експерту інформацію та враховувати як якісні так і кількісні фактори. На основі даного підходу було створено когнітивну модель, яка базуються на нечіткій когнітивній карті та дозволяє дослідити вплив потенційних загроз на рівень захищеності об'єкта критичної інфраструктури. Здійснено оцінювання структурно-топологічних властивостей нечіткої когнітивної карти, визначено її щільність, індекс ієрархії та центральність концептів. Із сформованої експертним шляхом множини концептів виділено найбільш вагомі. Проведено сценарне моделювання впливу даних концептів на захищеність об'єкта критичної інфраструктури. Дані отримані у результаті запуску відповідних сценаріїв дозволяють дослідити відносну зміну досліджуваної системи та сприяють ефективному вирішенню питань щодо підвищення рівня захищеності об'єктів критичної інфраструктури.*

Ключові слова: *інформаційна безпека, критична інфраструктура, загрози безпеці, когнітивне моделювання, нечітка когнітивна карта.*

Вступ

Стратегічно важливим для функціонування економіки і безпеки держави, суспільства та населення є захист об'єктів критичної інфраструктури (КІ) – підприємств та установ (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв [1]. У свою чергу, інформатизація об'єктів КІ викликає безліч ризиків, пов'язаних із порушенням функціонування інформаційних систем КІ, що може призвести до розвитку надзвичайних ситуацій, пов'язаних з великомасштабним порушенням життєдіяльності як окремих міст, так і усієї держави в цілому. Тому варто звернути особливу увагу на забезпечення інформаційної безпеки об'єктів КІ, враховуючи вплив потенційних загроз.

Вивчення даного питання відображається у роботах як українських, так і зарубіжних вчених. Зокрема, у роботі [2] розглянуто особливості забезпечення кібербезпеки об'єктів КІ. Автори роботи [3] здійснили аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкта КІ.

У роботі [4] запропоновано графічний та аналітичний методи оцінювання сумарного ризику кібербезпеки об'єктів КІ у результаті дії множини кіберзагроз.

Автором роботи [5] проаналізовано потенційні негативні наслідки, до яких може призвести кібератака на інформаційно-телекомунікаційну систему об'єкта КІ та запропоновано єдиний класифікатор таких наслідків.

У роботі [6] науковці розглянули принципи оцінювання ефективності дій зловмисника на об'єктах КІ та представили «операційний комплекс» моделювання процесів порушення інформаційної безпеки КІ.

Автори праці [7] запропонували нову технологію аналізу кіберзагроз та оцінювання ризиків порушення кібербезпеки КІ, що базується на використанні авторської інтелектуальної системи. Дана технологія включає етапи виявлення кіберзагроз; моделювання сценаріїв екстремальних ситуацій, викликаних реалізацією кіберзагроз; оцінювання ризиків і ранжування активів інформаційно-комунікаційної системи об'єкта КІ за ступенем їх критичності, і дозволяє виконати оцінювання кількості критично вразливих активів, обгрунтувати склад та ймовірність реалізації кіберзагроз.

Таким чином, значна увага приділяється дослідженням пов'язаним із забезпеченням безпеки об'єктів КІ при впливі на них ймовірних загроз. Причому дана задача характеризується високим ступенем невизначеності, складністю строгої формалізації та має суб'єктивний характер. Тому для її вирішення доцільно скористатися когнітивним підходом, який базується на побудові нечіткої когнітивної карти (НКК), тобто орієнтованого графа, вершини (концепти) якого представляють системні змінні, а зважені дуги відображають силу впливу одного концепта на інший [8]. У роботах [9] та [10] запропоновано когнітивні моделі, які дозволяють аналізувати вплив загроз на рівень захищеності комп'ютерної мережі та системи захисту інформації відповідно. Однак дані моделі є доволі вузькими, тому не можуть повною мірою відобразити предметну область КІ. Отже, актуальним є дослідження можливості побудови когнітивної моделі для оцінювання та прогнозування впливу потенційних загроз на рівень захищеності об'єкта КІ.

Мета роботи

Побудувати когнітивну модель для дослідження рівня захищеності об'єкта КІ.

Постановка задачі

Для досягнення поставленої мети необхідно:

– визначити структуру НКК предметної області (тобто склад її концептів та причинно-наслідкові зв'язки між ними);

– визначити силу впливу між кожною парою концептів;

– побудувати модель на основі НКК для дослідження рівня захищеності об'єкта КІ;

– визначити структурно-топологічні властивості розробленої НКК;

– визначити найвпливовіші концепти досліджуваної системи;

– провести сценарне моделювання для аналізу впливу найвагоміших загроз на рівень захищеності об'єкта КІ.

Побудова когнітивної моделі на основі НКК для дослідження рівня захищеності об'єкта КІ.

Дослідимо об'єкт КІ, який відноситься до класу об'єктів, що передбачає доступ до мережі Інтернет та відображає максимальне представлення структурних складових. Сформуємо множину загроз даному об'єкту, відмітивши, що основні напрями вектора атак направлені на ІТ-інфраструктуру та операційні технології [11]. Причому, велика кількість загроз спрямована на систему контролю та збору даних (SCADA) та на розподілені системи управління (DCS), які надають життєво важливі послуги КІ [12].

Доцільно виділити такі категорії загроз, на які має бути налаштовано захист КІ [13]:

– аварії й технічні збої, зокрема авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин, відмови систем, аварії та надзвичайні події, зумовлені недбалістю, організаційними помилками тощо;

– небезпечні природні явища, зокрема надзвичайні погодні умови, лісові, степові й торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища, урагани, торнадо, землетруси, цунамі, повені тощо;

– зловмисні дії, зокрема зловмисні дії груп або окремих осіб, таких як терористи, злочинці й диверсанти, а також бойові дії в умовах війни.

Особливо небезпечними є комбіновані загрози й загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів унаслідок взаємозалежності елементів КІ.

Загрози КІ можна розглядати не лише з огляду на характер їх походження, а й на елементи КІ, на які ці загрози спрямовані [13]:

– фізичні елементи, зокрема обладнання й ресурси об'єктів КІ;

– системи управління та комунікації, зокрема автоматизованих систем управління та систем зв'язку;

– персонал об'єктів, зокрема диспетчерський, оперативний, який безпосередньо забезпечує функціонування КІ у реальному часі.

У результаті проведення експертами аналізу можливих загроз безпеці КІ було сформовано множину найвагоміших, з точки зору вивчення даної проблеми, концептів:

– K_1 – природні явища;

– K_2 – техногенний вплив;

– K_3 – соціально-політичний вплив;

– K_4 – економічний вплив;

– K_5 – правовий вплив;

– K_6 – військове вторгнення;

– K_7 – терористичний вплив;

– K_8 – промислове шпигунство;

– K_9 – хакерський вплив;

– K_{10} – вплив управлінських рішень та організаційних заходів;

– K_{11} – інсайдерський вплив;

– K_{12} – безпека каналів зв'язку КІ;

– K_{13} – надійність, відмовостійкість складових КІ;

– K_{14} – захищеність КІ;

– K_{15} – захищеність системи безпеки;

– K_{16} – захищеність комп'ютерної мережі;

– K_{17} – безпека центру управління;

– K_{18} – безпека обслуговуючих систем та обладнання;

– K_{19} – безпека обслуговуючого персоналу;

– K_{20} – захищеність сховищ даних;

– K_{21} – захищеність хмарних серверів;

– K_{22} – безпека інформаційної інфраструктури;

– K_{23} – безпека Інтернет-додатків;

– K_{24} – безпека Інтернет;

– K_{25} – мережеві атаки;

– K_{26} – шкідливі програми;

– K_{27} – DoS-атаки.

Вплив загроз на K_{15} – захищеність системи безпеки та K_{16} – захищеність комп'ютерної мережі можна здійснювати на основі моделей, представлених у роботах [9, 10].

Наступним кроком є визначення сили впливу $w_{ij} \in [-1;1]$, що відображає зміни одного концепта K_i на зміну іншого K_j. Вирішення даної задачі здійснюється експертним шляхом за допомогою лінгвістичних термів та відповідних їм числових діапазонів.

Задамо нечітку лінгвістичну шкалу:

СИЛА ЗВ'ЯЗКУ = {Не впливає; Дуже слабка; Слабка; Середня; Сильна; Дуже сильна}.

Кожному з цих термів поставимо у відповідність деякий числовий діапазон:

$$w_{ij} = \begin{Bmatrix} (0{,}85;1], \ позитивна\ дуже\ сильна; \\ (0{,}6;0{,}85], \ позитивна\ сильна; \\ (0{,}35;0{,}6], \ позитивна\ середня; \\ (0{,}15;0{,}35], \ позитивна\ слабка; \\ (0;0{,}15], \ позитивна\ дуже\ слабка; \\ 0, \ не\ впливає; \\ (0;-0{,}15], \ негативна\ дуже\ слабка; \\ (-0{,}15;-0{,}35], \ негативна\ слабка; \\ (-0{,}35;-0{,}6], \ негативна\ середня; \\ (-0{,}6;-0{,}85], \ негативна\ сильна; \\ (-0{,}85;-1], \ негативна\ дуже\ сильна \end{Bmatrix}.$$

При позитивній силі зв'язку зростання концепта-причини призводить до збільшення концепта-наслідка, а при негативній – до зменшення.

Визначивши склад концептів та силу впливу причинно-наслідкових зв'язків між ними, побудуємо НКК для дослідження рівня захищеності об'єкта КІ (рис. 1).

Моделювання виконано з використанням засобів програмного забезпечення Mental Modeler [14].

Розглянемо матрицю $W = \left\lfloor w(K_i, K_j) \right\rfloor_{n \times n}$ взаємовпливів концептів даної НКК (табл. 1-2).

Визначимо структурно-топологічні властивості розробленої НКК, проаналізувавши такі показники структурної складності НКК як щільність, індекс ієрархії та центральність концептів:

а) щільність (коефіцієнт кластеризації) – показує ступінь зв'язності графа, який відображає дану НКК:

$$d = \frac{m}{n \cdot (n-1)}, \quad (1)$$

де m – загальна кількість зв'язків НКК, а n – загальна кількість концептів НКК.

У нашому випадку $n = 27$, $m = 128$, підставивши відповідні значення у формулу (1), отримаємо, що $d = 0{,}18$. Дане значення вказує на достатню складність розробленої моделі. Чим вище значення щільності, тим більше потенційних політик управління.

б) індекс ієрархії (h): $h = \frac{12 \cdot \sigma_{od}^2}{n^2 - 1}$, де

$$\sigma_{od}^2 = \frac{\sum_{i=1}^{n} (od_i - \mu_{od})^2}{n}, \ \mu_{od} = \frac{\sum_{i=1}^{n} od_i}{n}.$$

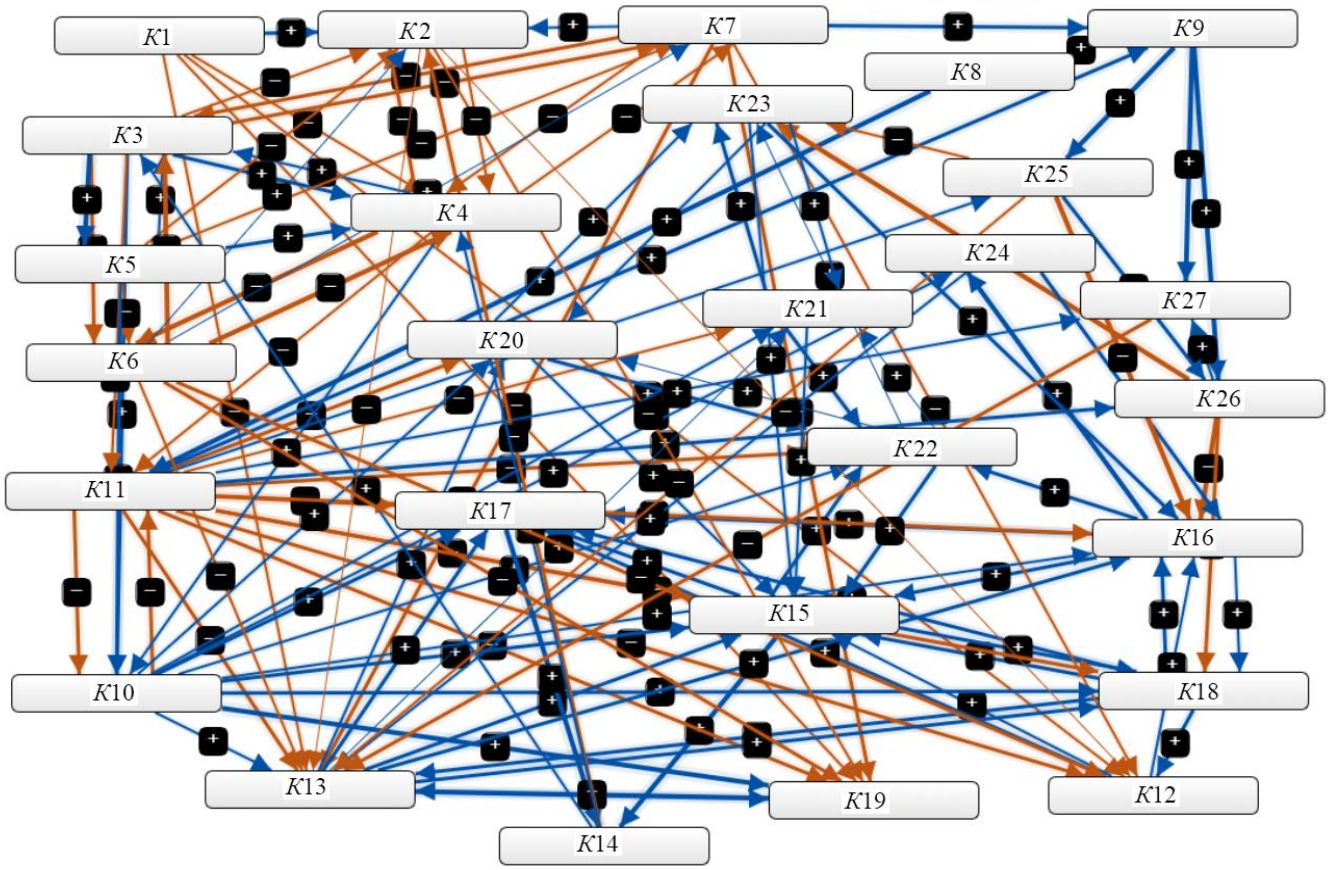

Рис. 1. НКК для дослідження рівня захищеності об'єкта КІ

Таблиця 1

Матриця взаємовпливів концептів НКК предметної області на концепти $K_1 - K_{15}$

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}
K_1	0	0,55	0	-0,4	0	0	0	0	0	0	0	-0,2	-0,3	0	0
K_2	0	0	0	-0,4	0	0	0	0	0	0	0	-0,1	-0,15	0	0
K_3	0	-0,35	0	0,7	0,85	-0,7	-0,5	0	0	0,75	-0,2	0	0	0	0
K_4	0	-0,5	0,3	0	0	-0,87	-0,4	0	0	0,35	-0,35	0	0	0	0
K_5	0	-0,4	0,4	0,55	0	-0,4	-0,4	0	0	0,8	-0,1	0	0	0	0
K_6	0	0,1	-0,85	-0,85	0	0	0,1	0	0	0	0	-0,5	-0,4	0	0
K_7	0	0,2	-0,5	-0,2	0	0	0	0	0,8	0	0	-0,3	-0,55	0	0
K_8	0	0	0	0	0	0	0	0	0,7	0	0,9	0	0	0	0
K_9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{10}	0	0	0	0	0	0	0	0	0	0	-0,7	0	0,2	0	0,7
K_{11}	0	0	0	0	0	0	0	0	0,8	-0,6	0	-0,6	-0,75	0	-0,8
K_{12}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,4
K_{13}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,55
K_{14}	0	-0,6	0,35	0,4	0	0	0	0	0	0	0	0	0	0	0
K_{15}	0	0	0	0	0	0	0	0	0	0	0	0	0	0,95	0
K_{16}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,5
K_{17}	0	0	0	0	0	0	0	0	0	0	0	0	0	0,95	0
K_{18}	0	0	0	0	0	0	0	0	0	0	0	0,7	0,5	0	0,8

K_{19}	0	0	0	0	0	0	0	0	0	0	0	0	0,7	0	0
K_{20}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,35
K_{21}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,35
K_{22}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,6
K_{23}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,4
K_{24}	0	0	0	0	0	0	0	0	0	0	0	0	0,35	0	0
K_{25}	0	0	0	0	0	0	0	0	0	0	0	0	-0,2	0	0
K_{26}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{27}	0	0	0	0	0	0	0	0	0	0	0	0	-0,6	0	0

Таблиця 2

Матриця взаємовпливів концептів НКК предметної області на концепти $K_{16} - K_{27}$

	K_{16}	K_{17}	K_{18}	K_{19}	K_{20}	K_{21}	K_{22}	K_{23}	K_{24}	K_{25}	K_{26}	K_{27}
K_1	0	0	0	-0,2	0	0	0	0	0	0	0	0
K_2	0	0	0	-0,4	0	0	0	0	0	0	0	0
K_3	0	0	0	0	0	0	0	0	0	0	0	0
K_4	0	0	0	0	0	0	0	0	0	0	0	0
K_5	0	0	0	0	0	0	0	0	0	0	0	0
K_6	0	0	0	-0,75	0	0	0	0	0	0	0	0
K_7	0	0	0	-0,55	0	0	0	0	0	0	0	0
K_8	0	0	0	0	0	0	0	0	0	0	0	0
K_9	0	0	0	0	0	0	0	0	0	0,9	0,9	0,9
K_{10}	0,4	0,7	0,6	0,9	0,4	0,2	0,25	0	0,4	0	0	0
K_{11}	-0,8	-0,8	-0,8	-0,6	-0,6	-0,4	-0,8	0	0	0,3	0,5	0,2
K_{12}	0,3	0,65	0	0	0	0	0	0	0	0	0	0
K_{13}	0,55	0,55	0,8	0,55	0,2	0,1	0	0	0	0	0	0
K_{14}	0	0	0	0	0	0	0	0	0	0	0	0
K_{15}	0	0,8	0,6	0	0	0	0,6	0	0	0	0	0
K_{16}	0	0,6	0,4	0	0	0	0,7	0	0,85	0	0	0
K_{17}	0	0	0	0	0	0	0	0	0	0	0	0
K_{18}	0,8	0,8	0	0	0	0	0	0	0	0	0	0
K_{19}	0	0	0	0	0	0	0	0	0	0	0	0
K_{20}	0	0	0	0	0	0	0,8	0,4	0	0	0	0
K_{21}	0	0	0	0	0	0	0,55	0,8	0	0	0	0
K_{22}	0	0	0	0	0,15	0,1	0	0,1	0	0	0	0
K_{23}	0,75	0	0	0	0,3	0,2	0	0	0	0	0	0
K_{24}	0,75	0	0	0	0	0	0	0	0	0	0	0
K_{25}	-0,9	0	0	0	0	0	0	-0,25	0	0	0,7	0
K_{26}	-0,9	0	-0,65	0	0	0	0	-0,85	0	0	0	0,2
K_{27}	0	0	0	0	0	0	0	0	0	0	0	0

При $h=1$ система є повністю ієрархічною, при $h=0$ – повністю демократичною. Демократичні системи більш адаптивні до змін зовнішнього середовища завдяки високому рівню їх інтеграції та зв'язності. У нашому випадку $\mu_{od}=2{,}51,\quad \sigma^2_{od}=3{,}13$, тоді $h=0{,}16$, що свідчить про високу демократичність досліджуваної системи.

в) центральність концепта – характеризує ступінь взаємодії і-го концепта НКК з його сусідами:

– вихідна центральність – показує сукупну силу зв'язків (w_{ij}), що виходять з аналізованого концепта K_i:

$$od_i=\sum_{j=1}^{n} w_{ij};$$

– вхідна центральність – показує сукупну силу зв'язків (w_{ij}), що входять до аналізованого концепта K_i:

$$id_i=\sum_{j=1}^{n} w_{ij};$$

– загальна центральність концепта: $td_i=od_i+id_i.$

Розрахунок показників центральності показав, що найбільш високу структурну значимість має концепт K_{11} $(td_i=11{,}6)$, а також концепти $K_{16}, K_{15}, K_{13}, K_{10}$ (показники $td_{16,}\ td_{15}, td_{13}, td_{10}$ рівні відповідно 9,2; 8,39; 8,0; 7,95). Дані концепти акумулюють найбільшу кількість зв'язків від інших концептів, тобто відіграють роль своєрідних центрів впливу у НКК для дослідження рівня захищеності об'єкта КІ. Зазначимо, що найменшу структурну значимість відіграє концепт K_8 $(td_i=1{,}6)$.

Сценарне моделювання для оцінювання впливу найвагоміших загроз на рівень захищеності об'єкта КІ.

Сценарний аналіз дозволяє отримати прогноз розвитку досліджуваної ситуації, визначити, оцінити і знизити рівень невизначеності впливу найвагоміших концептів, що впливають на захищеність об'єкта КІ. Це, у свою чергу, сприятиме формуванню стратегічних управлінських рішень щодо підсилення захисту об'єкта КІ. Метод побудови сценаріїв найбільш повно дозволяє проаналізувати вплив найвагоміших загроз на рівень захищеності об'єкта КІ в умовах невизначеності та мінливості оточуючого середовища.

Сценарій 1. Змоделюємо ситуацію, при якій спостерігатиметься максимальне збільшення інсайдерського впливу (K_{11}) на захищеність об'єкта КІ.

Зауважимо, що численні дослідження, проведені у останні роки, показують, що більше 80% усіх інцидентів, пов'язаних з порушенням інформаційної безпеки, викликані внутрішніми загрозами. Джерелами таких загроз, що спричиняють порушення конфіденційності інформації, є, як правило, інсайдери, тобто особи, що мають через свій службовий стан доступ до інформації обмеженого доступу або ж співробітники, які намагаються його отримати [15].

При максимальному інсайдерському впливі спостерігатиметься така реакція досліджуваної системи (рис. 2).

Аналізуючи отриману стовпчасту діаграму можна зробити висновок, що найбільше зменшиться значення концептів K_{16} – захищеність комп'ютерної мережі (на 0,24) та K_{18} – безпека обслуговуючих систем та обладнання (на 0,21). Крім того, значно погіршиться K_{13} – надійність, відмовостійкість складових КІ (на 0,17), K_{22} – безпека інформаційної інфраструктури (на 0,16), K_{17} – безпека центру управління (на 0,14), K_{19} – безпека обслуговуючого персоналу (на 0,13), K_{12} – безпека каналів зв'язку КІ (на 0,12), K_{15} – захищеність системи безпеки (на 0,12) та K_{20} – захищеність сховищ даних (на 0,12). Проте K_{14} – захищеність КІ послабиться лише на 0,03.

Для попередження негативних наслідків необхідно особливу увагу приділяти основним компонентам комплексної системи організованих заходів й технічних засобів захисту від інсайдерів, а саме [16]:

– нормативно-правовій базі;

– системі контролю та управління персоналізованим доступом до корпоративних ресурсів КІ;

– моніторингу дій користувачів інформації;

– використанню технічних засобів, що здійснюють контроль й очистку комп'ютерних систем;

– кадровому забезпеченню (обов'язкова наявність штатного спеціаліста, що забезпечує захист від внутрішніх загроз);

– забезпеченню відповідного рівня корпоративної культури, що впливає на підвищення рівня корпоративної безпеки КІ;

– ретельній підбір кадрів, що матимуть доступ до інсайдерської інформації;

– формування ефективного мотиваційного механізму для працівників.

Реалізація зазначених заходів допоможе зменшити інсайдерський вплив та підвищити рівень захищеності КІ.

Сценарій 2. Розглянемо як зміниться стан досліджуваної системи при максимальному послабленні концепта K_{16} – захищеність комп'ютерної мережі.

Відмітимо, що комп'ютерна мережа є базисом для функціонування інформаційних систем у різних сегментах діяльності об'єкта КІ. Адже вона забезпечує передавання даних і комунікацію між автоматизованими вузлами даного об'єкта, управління правами доступу до інформаційних ресурсів і безпосередньо впливає на ефективне впровадження та застосування інформаційних технологій. Тому цікаво змоделювати даний сценарій для аналізу відносної зміни рівня системи (рис. 3).

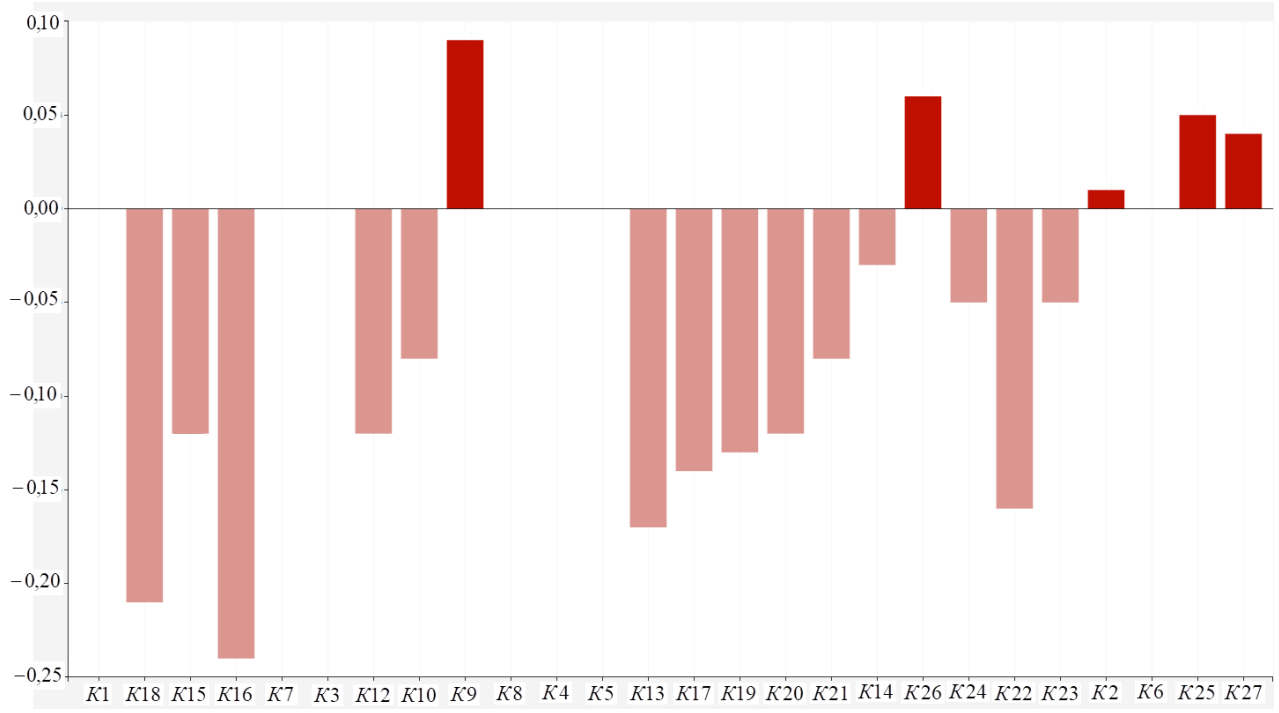

Рис. 2. Реакція досліджуваної системи на максимальний інсайдерський вплив

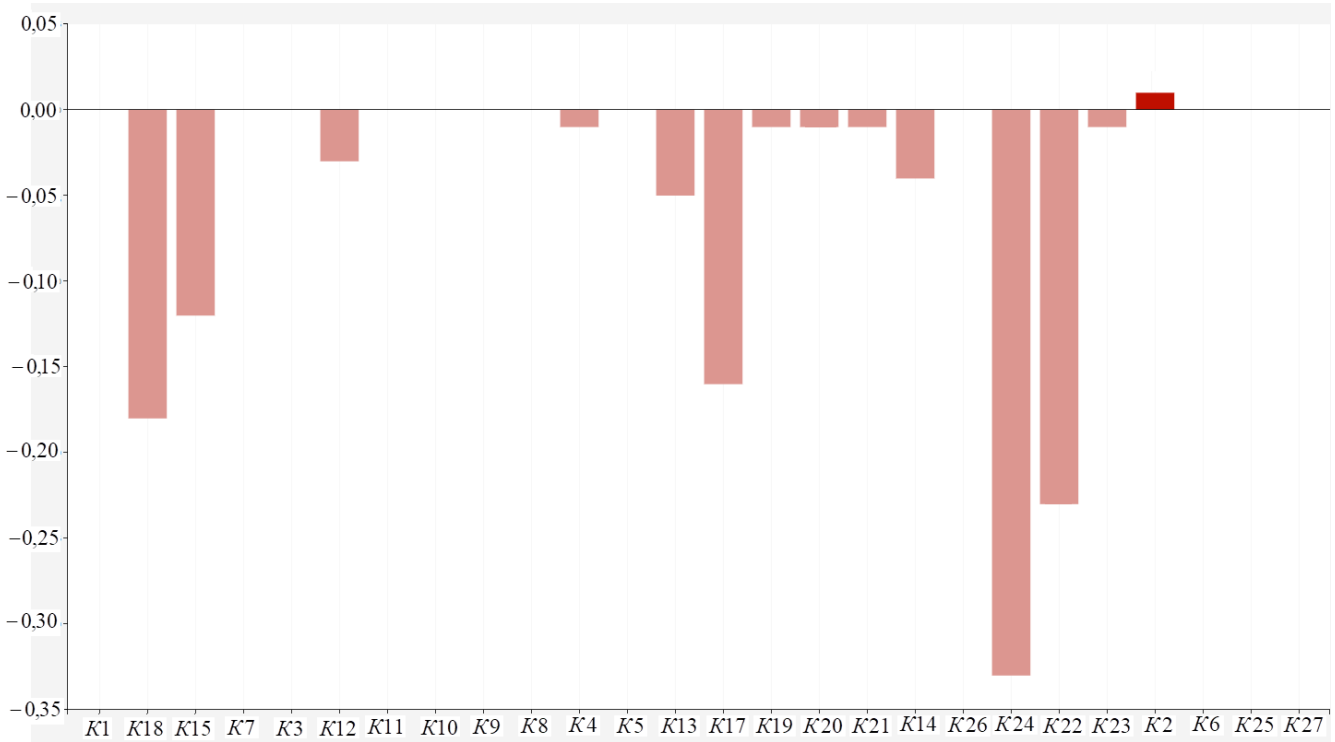

Рис. 3. Реакція досліджуваної системи при максимальному послабленні захисту комп'ютерної мережі

Дослідивши отриману гістограму, можна зробити висновок, що при максимальному послабленні захисту комп'ютерної мережі найбільше зменшаться значення концептів: K_{24} – безпека Інтернет (на 0,33), K_{18} – безпека обслуговуючих систем та обладнання (на 0,28), K_{22} – безпека інформаційної інфраструктури (на 0,25), K_{17} – безпека центру управління (на 0,24) та K_{15} – захищеність системи безпеки (на 0,18). Значення інших концептів системи зміняться не суттєво. При цьому K_{14} – захищеність КІ послабиться на 0,06.

Щоб запобігти вищезазначеним негативним наслідкам необхідно впроваджувати та застосовувати ефективні механізми і засоби для забезпечення мережевої безпеки на об'єктах КІ, які захищатимуть мережу від несанкціонованого доступу, випадкового або навмисного втручання у її роботу або спроб руйнування її компонентів.

Сценарій 3. Змоделюємо ситуацію, яка відображатиме зміни концептів системи при максимально можливому послабленні захищеності системи безпеки.

Основною метою створення системи безпеки на об'єктах КІ є попередження та нейтралізація загроз, реалізація яких може призвести до порушення функціонування складових КІ, що, у свою чергу, може негативно вплинути на загальнодержавну, екологічну та суспільну безпеку. Дана система проводить комплексні адміністративно-правові, інформаційно-аналітичні, організаційно-управлінські, та інші заходи, спрямовані на забезпечення стійкого функціонування об'єктів КІ.

Розглянемо реакцію досліджуваної системи на максимально негативну зміну концепта K_{15} – захищеність системи безпеки (рис. 4).

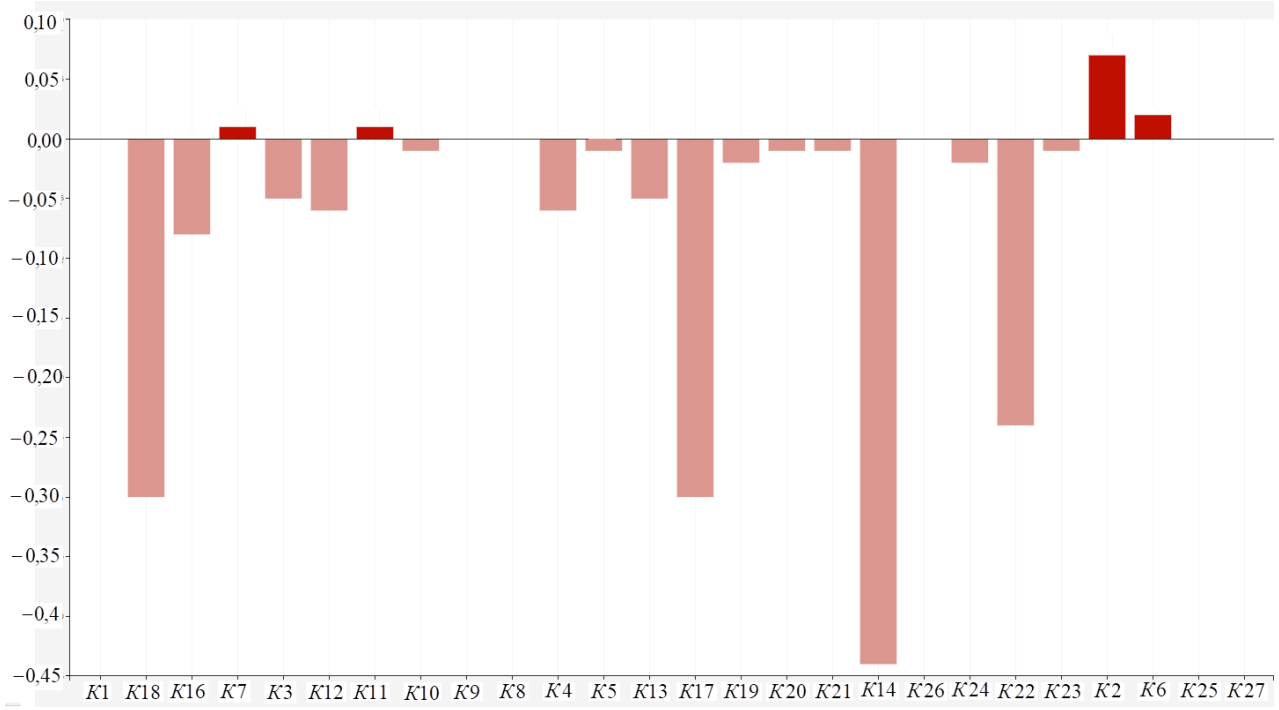

Рис. 4. Реакція досліджуваної системи при максимальному послабленні захищеності системи безпеки

Проаналізувавши отриману стовпчасту діаграму, можна зробити висновок, що при максимальному послабленні захищеності системи безпеки спостерігатиметься найбільша вразливість захищеності критичної інфраструктури, адже значення даного концепта знизиться на 0,44. При цьому безпека інформаційної інфраструктури (K_{22}) послабиться на 0,24, а безпека обслуговуючих систем та обладнання (K_{18}) і безпека центру управління (K_{17}) – кожна на 0,3. Для попередження даної ситуації необхідно особливу увагу приділити захищеності системи безпеки, послаблення якої може призвести до вкрай негативних наслідків функціонування об'єктів КІ, що у результаті спровокує небезпечний вплив на навколишнє середовище та людство в цілому.

Таким чином, розроблена когнітивна модель для дослідження рівня захищеності об'єкта КІ дозволяє прослідкувати відносну зміну досліджуваної системи на зміни тих чи інших концептів, визначивши найвагоміші з них. На основі результатів сценарного моделювання можна розробити чіткий план управління спрямований на підвищення захищеності об'єктів КІ, які є стратегічно важливими для розвитку держави.

Висновки

Побудовано когнітивну модель дослідження рівня захищеності об'єкта КІ. На основі проведеного аналізу показників структурної складності НКК, визначено структурно-топологічні властивості розробленої моделі. Встановлено значення коефіцієнта кластеризації НКК ($d = 0{,}18$), яке свідчить про достатню складність розробленої моделі. Визначено індекс ієрархії ($h = 0{,}16$), що відображає високу демократичність досліджуваної системи. Розраховано показники центральності, за допомогою яких встановлено, що найбільш високу структурну значимість має концепт K_{11} ($td_i = 11{,}6$), а також концепти K_{16}, K_{15}, K_{13}, K_{10} (показники центральності яких відповідно рівні 9,2; 8,39; 8,0; 7,95).

Проведено сценарне моделювання для визначення відносної зміни досліджуваної системи при максимально негативному впливі найвагоміших концептів. Проаналізувавши отримані результати, можна зробити висновок, що захищеність КІ максимально знизиться (на 0,44) якщо найбільшою мірою послабиться захищеність системи безпеки. При зростанні інсайдерського впливу спостерігатиметься, у першу чергу, погіршення захищеності комп'ютерної мережі (на 0,24) та безпеки обслуговуючих систем та обладнання (на 0,21). У свою чергу, при максимальному послабленні захисту комп'ютерної мережі найбільше знизиться безпека Інтернет (на 0,33), безпека обслуговуючих систем та обладнання (на 0,28), безпека інформаційної інфраструктури (на 0,25) та безпека центру управління (на 0,24).

На основі аналізу отриманих даних можна запобігти порушенню режимів функціонування ключових елементів об'єктів КІ, що, у свою чергу, може призвести до розвитку надзвичайних ситуацій, здатних паралізувати життєдіяльність як окремих міст, так і усієї держави в цілому.

Література

[1]. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова КМУ від 23.08.2016 р. № 563 . *Офіційний вісник України*. 2016. №69.

[2]. С. Гончар, "Особливості забезпечення кібербезпеки об'єктів критичної інфраструктури", *Моделювання та інформаційні технології*, Вип. 80, С. 27-32, 2017.

[3]. С. Гончар, Г. Леоненко, "Аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури", *Information technology and security*, Vol. 4, issue 2 (7), С. 262-268, 2016.

[4]. В. Мохор, С. Гончар, О. Дибач, "Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури", *Ядерна та радіаційна безпека*, Вип. 2, С. 4-8, 2019.

[5]. Ю. Дрейс, "Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави", *Захист інформації*, Т. 19, № 3, С. 214-222, 2017.

[6]. И. Горбачев, А. Глухов, "Моделирование процессов нарушения информационной безопасности критической инфраструктуры", *Тр. СПИИ РАН*, Вып. 1 (38), С. 112–135, 2015.

[7]. Д. Гаськова, А. Массель, "Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры", *Вопросы кибербезопасности*, №2(30), С. 42-49, 2019.

[8]. B. Kosko, "Fuzzy Cognitive Maps", *International Journal of Man-Machine Studies*, Vol. 24, No. 1, pp. 65-75, 1986.

[9]. О. Салієва, Ю. Яремчук, "Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі", *Реєстрація, зберігання і обробка даних*, №4, С. 28–39, 2019.

[10]. О. Салієва, Ю. Яремчук, "Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання", *Безпека інформації*, №1, С. 42-49, 2020.

[11]. А. Массель, Д. Гаськова, "Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов", *Онтология проектирования*, Т. 9, №2(32), С. 225-238, 2019.

[12]. A. Leandros, K. Ki-Hyung, J. Helge, "Cruz Cyber security of critical infrastructures", *ICT Express*, №4, pp. 42-45, 2018.

[13]. Д. Бірюков, С. Кондратов, О. Суходоля, *Зелена книга з питань захисту критичної інфраструктури в Україні*, К., 2016, 176 с.

[14]. S. Gray, J. De Kok, A.E.R. Helfgott, B. O'Dwyer, R. Jordan, A. Nyaki, "Using fuzzy cognitive mapping as a participatory approach to analyze change, preferred states, and perceived resilience of social-ecological sys-tems", *Ecology and Society*, 20(2):11, 2015. [Electronic resource]. Online access: http://www. ecologyandsociety. org/vol20/iss2/art11.

[15]. В. Козюра, В. Хорошко, "Заходи протидії прихованої передачі інформації в локальних мережах. Актуальні проблеми управління інформаційною безпекою держави", *зб. тез наук. доп. наук.-практ. конф., Київ : Нац. акад. СБУ*, С. 91-93, 2018.

[16]. В. Малащенко, "Теоретичні підходи до проблем та сучасних способів захисту від «інсайдерів»", *Ефективність державного управління*, Вип. 29, 2011. [Електронний ресурс]. Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/Edu/2011_29/fail/malashchenko.pdf.

УДК 004.056.53

Салиева О.В., Яремчук Ю.Е. Когнитивная модель для исследования уровня защищенности объекта критической инфраструктуры

Аннотация. *Для решения вопросов по обеспечению защищенности объектов критической инфраструктуры необходимо проанализировать потенциальные угрозы, исследовать взаимосвязи между ними и определить влияние данных угроз на исследуемую систему. При этом появляются некоторые трудности связаны с высокой степенью неопределенности, сложности строгой формализации и субъективным характером данных задач. В связи с этим в работе предлагается использование когнитивного подхода, который не требует большого объема экспериментальных данных, дает возможность обрабатывать доступную экспертную информацию и учитывать, как качественные, так и количественные факторы. На основе данного подхода была создана когнитивная модель, которая основанная на нечеткой когнитивной карте и позволяет проанализировать влияние потенциальных угроз на уровень защищенности объектов критической инфраструктуры. Осуществлено оценивания структурно-топологических свойств нечеткой когнитивной карты, определены ее плотность, индекс иерархии и центральность концептов. С множества концептов выделены наиболее весомые. Проведено сценарное моделирование влияния данных концептов на защищенность объектов критической инфраструктуры. Данные получены в результате запуска соответствующих сценариев позволяют исследовать относительное изменение исследуемой системы и способствуют эффективному решению вопросов по повышению уровня защищенности объектов критической инфраструктуры.*

Ключевые слова: *информационная безопасность, критическая инфраструктура, угрозы безопасности, когнитивное моделирование, нечеткая когнитивная карта.*

Saliieva O., Yaremchuk Yu. Cognitive model for studying the level of protection of a critical infrastructure object
Abstract*. The protection of critical infrastructure is strategically important for the functioning of the economy and security of the state, society and the population. To address the protection of critical infrastructure, it is necessary to analyze potential threats, explore the relationships between them and determine the impact of these threats on the system under study. However, there are some difficulties associated with a high degree of uncertainty, the complexity of strict formalization and the subjective nature of these tasks. In this regard, the paper proposes the use of a cognitive approach, which does not require a large amount of experimental data, provides an opportunity to process the information available to the expert and take into account both qualitative and quantitative factors. Based on this approach, a cognitive model was created, which is based on a fuzzy cognitive map and allows to study the impact of potential threats on the level of protection of critical infrastructure. To build a fuzzy cognitive map, many of the most important critical infrastructure threats from the point of view of this problem have been formed and causal links have been established between them. The evaluation of structural and topological properties of fuzzy cognitive map is carried out, its density, hierarchy index and centrality of concepts are determined. From the set of expertly formed set of concepts, the most important ones are selected. To determine the relative change in the level of protection of the critical infrastructure, a scenario modeling of the impact of the most important concepts on the studied system was performed. Based on the analysis of the data obtained as a result of the launch of appropriate scenarios, it is possible to prevent disruption of key elements of critical infrastructure, which, in turn, can lead to emergencies that can paralyze the lives of individual cities and the state as a whole.*
Keywords: *information security, critical infrastructure, security threats, cognitive modeling, fuzzy cognitive map.*

Салієва Ольга Володимирівна, аспірантка кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.
Салиева Ольга Владимировна, аспирантка кафедры менеджмента и безопасности информационных систем Винницкого национального технического университета.
Saliieva Olha, graduate student of the Department of Management and Security of Information Systems, Vinnytsia National Technical University.

Яремчук Юрій Євгенович, директор Центру інформаційних технологій та захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.
Яремчук Юрий Евгеньевич, директор Центра информационных технологий и защиты информации, профессор кафедры менеджмента и безопасности информационных систем Винницкого национального технического университета.
Yaremchuk Yurii, Director of the Center for Information Technologies and Information Protection, Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University.

Отримано *15 липня 2020 року*, затверджено редколегією *10 серпня 2020 року*