УДК 004.056

Дудатьєв А. В.[1], Войтович О. П.[2]

[1]Канд. техн. наук, доцент, доцент кафедри захисту інформації Вінницького Національного Технічного Університету, Вінниця, Україна

[2]Канд. техн. наук, доцент, доцент кафедри захисту інформації Вінницького Національного Технічного Університету, Вінниця, Україна

МОДЕЛІ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ УПРАВЛІННЯ КОМПЛЕКСНОЮ ІНФОРМАЦІЙОНОЮ БЕЗПЕКОЮ

Актуальність. Існування конкурентного інформаційного середовища, яке є специфічною ареною для проведення спеціальних інформаційних операцій показує на необхідність реалізації комплексного захисту інформаційних ресурсів. Перебіг інформаційної війни, а також проблеми, що виникають при управлінні комплексною інформаційною безпекою визначає актуальність розробки моделей інформаційної підтримки прийняття рішень та створення ситуаційних або інформаційно-аналітичних центрів управління комплексною інформаційною безпекою на рівні «підприємство – регіон – держава».

Мета. Метою даного дослідження є розробка моделі інформаційної підтримки прийняття рішень управління комплексною інформаційною безпекою багаторівневої соціотехнічної системи у складі окремих об'єктів, групи об'єктів (регіону) та держави в цілому, що дозволить отримати кількісні показники рівня захищеності системи з можливістю прийняття рішень щодо управління комплексною інформаційною безпекою на рівнях «підприємство – регіон – держава».

Метод. Метод дослідження будується на ідеї того, що рівень захищеності держави залежить від рівня захищеності підпорядкованих регіонів, рівень захищеності яких, у свою чергу, залежить від рівня захищеності підпорядкованих локальних об'єктів. Рівень захищеності самого підприємства залежить від порушення хоча б одного з критеріїв: цілісності, доступності, конфіденційності.

Результати. Вирішено задачу розробки узагальненої моделі оцінювання комплексної інформаційної безпеки багаторівневої соціотехнічної системи типу «підприємство – регіон – держава», що дозволяє отримати оцінку рівня інформаційної захищеності, як локального об'єкта – підприємства, так і інтегрованих об'єктів – регіону та держави. Для оцінювання ймовірностей виникнення базових загроз можуть бути використані ймовірнісні оцінки або експертні оцінки, які представлені у вигляді нечітких множин. Запропоновано структурну модель багаторівневого інформаційно-аналітичного центру управління комплексною інформаційною безпекою. Результати проведених досліджень показали можливість використання даного підходу для рішення задач оцінювання та управління комплексною інформаційною безпекою багаторівневої соціотехнічної системи.

Висновки. Наукова новизна проведеного дослідження полягає в тому, що вперше запропоновано модель оцінювання комплексної інформаційної безпеки багаторівневої соціотехнічної системи на рівнях управління «підприємство – регіон – держава».

Практична новизна полягає у розробці програмного забезпечення, яке реалізує процес аналізу та оцінювання рівня комплексної інформаційної захищеності багаторівневої соціотехнічної системи на рівнях управління «підприємство – регіон – держава», а також синтезу управлінських рішень на базі сформованих баз знань.

Ключові слова: соціотехнічна система, комплексна інформаційна безпека, інформаційна війна, спеціальні інформаційні операції, інформаційно-аналітичний центр, підтримка прийняття рішень.

НОМЕНКЛАТУРА

АС – автоматизована система;

ІАЦ –- інформаційно-аналітичного центру;

ІКО – інформаційно-кібернетична операція;

ІПО – інформаційно-психологічна операція;

СТС – соціотехнічна система;

A – нечітке число;

B – нечітке число;

f – логіко-ймовірнісна операція;

F – логіко-ймовірнісна операція;

m – найбільш достовірне значення нечіткого числа;

n – кількість загроз;

P_{x_i} – ймовірність виникнення загрози для окремого об'єкта захисту;

x – вхідна загроза для окремого об'єкта захисту або підприємства;

$\tilde{x}_i$ – значення елемента нечіткої множини;

X – множина вхідних загроз для окремого об'єкта захисту або підприємства;

y – рівень захищеності локального об'єкта або підприємства;

Y – множина вхідних загроз для окремого регіону;

Y_{der} – рівень захищеності держави;

Y_{reg} – рівень захищеності окремого регіону;

Y_{rz} – множина вхідних загроз для держави;

α – відхилення зліва нечіткого числа;

β – відхилення справа нечіткого числа;

μ – функція приналежності;

φ – логіко-ймовірнісна операція.

ВСТУП

Життєдіяльність сучасних виробничих, економічних, технічних та інших систем, які можна віднести до класу СТС, відбувається в різних конкурентних середовищах, в тому числі, конкурентному інформаційному просторі, що є специфічною ареною для проведення спеціальних інформаційних операцій. Оскільки останні проводяться проти СТС, тобто проводяться або проти соціальної частини СТС у вигляді спеціальних ІПО або проти технічної частини СТС у вигляді спеціальних ІКО, то і процес побудови систем захисту повинен бути комплексним. Спеціальні інформаційні операції можуть проводитися на різних рівнях управління комплексною інформаційною безпекою: рівні одного підприємства, групи підприємств або цілої галузі промисловості, того чи іншого регіону та нарешті держави в цілому. Причому, ефективно проведені спеціальні інформаційні операції проти так званих критичних об'єктів, наприклад, енергетичних

DOI 10.15588/1607-3274-2017-1-13

об'єктів, в першу чергу АЕС, хімічно небезпечних об'єктів, спеціальні інформаційні операції проведені на транспорті можуть призвести до ризиків регіонального, державного і загальносвітового масштабів.

Перебіг інформаційної війни супроводжується збільшенням кількості засобів і методів ведення деструктивних інформаційних впливів, постійною трансформацією загроз які супроводжують проведення спеціальних інформаційних операцій. Про це свідчить збільшення кількості інцидентів на різних рівнях управління інформаційною безпекою в різних регіонах світу. Крім того виникає низка специфічних проблем, ефективне рішення яких можливо лише за умови реалізації системного підходу, який полягає у побудові власної цілісної системи комплексного захисту інформаційних ресурсів. Це пов'язано з [1]:

– ускладненням та розширенням кола задач управління інформаційною безпекою.

– підвищенням вимог до оперативності та якості прийняття і реалізації управлінських рішень;

– високою мірою відповідальності за прийняте рішення;

– необхідністю в довгостроковому і короткостроковому прогнозуванні розвитку ситуації;

– необхідністю ефективного реагування на швидкі зміни ситуації;

– необхідністю оцінювання ризиків та загроз;

– необхідністю прийняття оптимальних і обґрунтованих рішень.

Саме тому існує нагальна потреба рішення актуальної задачі розробки моделей інформаційної підтримки та створення ситуаційних або ІАЦ управління комплексною інформаційною безпекою на рівні «підприємство – регіон – держава».

Об'єктом дослідження є процес побудови моделей інформаційної підтримки управління комплексною інформаційною безпекою багаторівневих соціотехнічних систем на базі логіко-ймовірнісних моделей.

Предметом дослідження є моделі та структури ІАЦ прийняття рішень управління комплексною інформаційною безпекою.

Метою даного дослідження є розробка моделі інформаційної підтримки прийняття рішень управління комплексною інформаційною безпекою багаторівневою СТС у складі окремих об'єктів, групи об'єктів або регіону та держави в цілому, що дозволить отримати кількісні показники рівня захищеності системи з можливістю прийняття рішень щодо управління комплексною інформаційною безпекою на рінях «підприємство – регіон – держава».

Для досягнення поставленої мети необхідно вирішити такі задачі:

1. Розробити узагальнену математичну модель для оцінювання рівня комплексної інформаційної безпеки багаторівневої системи «підприємство – регіон – держава».

2. Розробити структурну модель багаторівневого ІАЦ управління комплексною інформаційною безпекою.

3. Розробити програмний засіб для інформаційної підтримки прийняття рішень щодо управління комплексною інформаційною безпекою.

1 ПОСТАНОВА ЗАДАЧІ

Нехай маємо множину базових загроз інформаційній безпеці для окремого об'єкта захисту $X = \{x_1, x_2, ..., x_n\}$ та ймовірності виникнення даних загроз, які можуть бути визначені, як ймовірностями їх виникнення $\{P_{x_1}, P_{x_2}, ..., P_{x_n}\}$, так і експертними оцінками, які формалізуються нечіткою множиною, яка подана у вигляді трійки значень $A = (m_A, \alpha_A, \beta_A)$.

Тоді задача розробки інтегрованої математичної моделі оцінювання рівня захищеності багаторівневої соціотехнічної системи буде полягати у побудові інтегрованої логіко-ймовірнісної моделі, яка об'єднує різні рівні управління.

Для оцінки адекватності запропонованої моделі потрібно проведення комп'ютерного експерименту з реальними об'єктами захисту – підприємствами, які складають умовний регіон.

2 ОГЛЯД ЛІТЕРАТУРИ

25 січня 2015 року Президент України Петро Порошенко ввів у дію рішення РНБО про створення та забезпечення діяльності Головного ситуаційного центру України, до якого надходитиме від державних служб і правлінь інформація з обмеженим доступом. Згідно з рішенням РНБО, Головний ситуаційний центр функціонуватиме як програмно-апаратний комплекс зі збору, накопичення й обробки інформації, необхідної для підготовки та прийняття рішень у сфері національної безпеки і оборони [2]. Оскільки інформаційна безпека є важливою складовою національної безпеки то створення ІАЦ управління комплексною інформаційною безпекою, як складової Головного ситуаційного центру має бути невід'ємною частиною щодо реалізації рішення РНБО.

Відомі теоретичні розробки математичних моделей для оцінювання інформаційних ризиків, а також структурних моделей ІАЦ. Відомими роботами в даній області є дослідження вітчизняних та зарубіжних вчених, таких як: Корченко О. Г., Архипов О. Є., Ільїн М. І., Дємідов М. М. [1, 3, 4]. Однак запропоновані моделі не дозволяють отримати оцінку комплексної інформаційної безпеки багаторівневих соціотехнічних систем з урахуванням умов ведення інформаційної війни.

У роботі [4] наведені структури ІАЦ управління різними технологічними процесами багаторівневих систем, але не враховуються особливості побудови ІАЦ для управління комплексною інформаційною безпекою. Структура ІАЦ на прикладі системи «підприємство – держава» розглянута у роботі [5], проте в ній відсутні математичні моделі підтримки прийняття рішень, а акцент зроблений на класифікацію різних критичних систем. Методи та моделі збирання, оброблення та прийняття рішень у ситуаційних центрах на локальному рівні описані у [6, 7] без врахування особливостей багаторівневого підходу на рівні «підприємство – регіон – держава». Для вирішення задачі оцінювання захищеності інформаційних ресурсів на рівні «підприємство – регіон – держава», з урахуванням структури локальних об'єктів або окремих підприємств, структури регіону, можливих

шляхів доступу зловмисників до ресурсів та проведення спеціальних інформаційних операцій використано логіко-ймовірнісну модель. Такий підхід дозволяє відстежити причинно-наслідкові зв'язки початку, розвитку і закінчення проведення спеціальних інформаційних операцій і реалізації інших загроз [8].

3 МАТЕРІАЛИ ТА МЕТОДИ

Загальна математична модель оцінювання та забезпечення рівня комплексної інформаційної безпеки багаторівневої системи будується на ідеї того, що рівень захищеності держави залежить від стану захищеності підпорядкованих регіонів, рівень захищеності яких, у свою чергу, залежить від стану рівня комплексної інформаційної захищеності підпорядкованих локальних об'єктів. Стан захищеності самого підприємства залежить від порушення хоча б одного з критеріїв: цілісності, доступності, конфіденційності. Іншими словами, кожне підприємство розглядається, як окрема загроза для відповідного регіону, який об'єднує певну кількість об'єктів захисту, а кожний регіон розглядається, як окрема загроза для держави. Такий підхід надасть можливість використання єдиної інтегрованої логіко-ймовірнісної моделі, яка формалізує всі процеси ймовірних порушень комплексної інформаційної безпеки на відповідних рівнях управління від окремого підприємства до держави.

На локальних об'єктах, або окремих підприємствах, рівень захищеності можна представити такою аналітичною залежністю:

$$y = f(x_1, x_2, ..., x_n), \quad (1)$$

де $X = \{x_1, x_2, ..., x_n\}$ – множина вхідних загроз для окремого об'єкта захисту або підприємства.

Для рівня комплексної безпеки регіону, який об'єднує декілька підприємств, пропонується така залежність:

$$Y_{reg} = \varphi(y_1, y_2, ..., y_n), \quad (2)$$

де $Y = \{y_1, y_2, ..., y_n\}$ – множина вхідних загроз для окремого регіону, які фактично представляють рівні захищеності окремих підприємств, що входять в даний регіон. На державному рівні управління комплексною інформаційною безпекою, зв'язок вихідних параметрів з вхідними представляється такою залежністю:

$$Y_{der} = F(Yreg_1, Yreg_2, ..., Yreg_n), \quad (3)$$

де $Y_{rz} = \{Y_{reg_1}, Y_{reg_2}, ..., Y_{reg_n}\}$ – множина вхідних загроз для держави, які фактично представляють рівні захищеності окремих регіонів. Таким чином узагальнену модель оцінювання рівня комплексної інформаційної безпеки багаторівневої структури «підприємство – регіон – держава» можна представити, як перетворення:

$$Y_{der} = F(\varphi(f(x_1, x_2, ...x_n))). \quad (4)$$

Структурна модель ІАЦ управління комплексною інформаційною безпекою, яка відповідає аналітичній моделі (4) представлена на рис. 1.

Структурна модель включає зворотні зв'язки на рівні ІАЦ регіону і ІАЦ держави, які дозволять корегувати управлінські рішення на відповідному рівні. Крім того зворотній зв'язок дозволить організувати і підтримувати базу знань. Сформована база знань дозволяє генерувати правила трьохрівневої політики безпеки, які відповідають поточній безпековій ситуації і мінімізувати ймовірні ризики реалізації зовнішнього керованого хаосу за рахунок самоорганізації системи. Фрагмент логіко-ймовірнісної моделі для оцінювання порушення рівня інформаційної безпеки держави, поданої у вигляді дерева-подій, наведено на рис. 2.

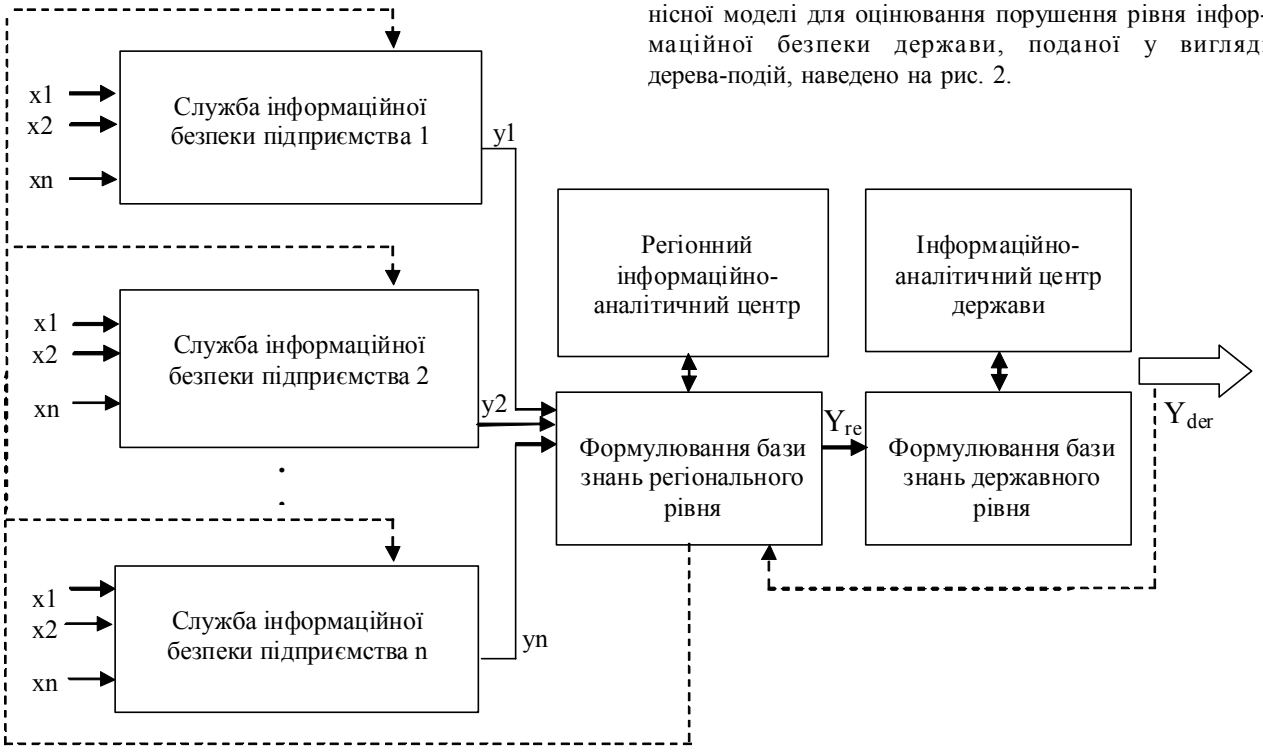

Рисунок 1 – Структурна модель багаторівневого ІАЦ управління комплексною інформаційною безпекою

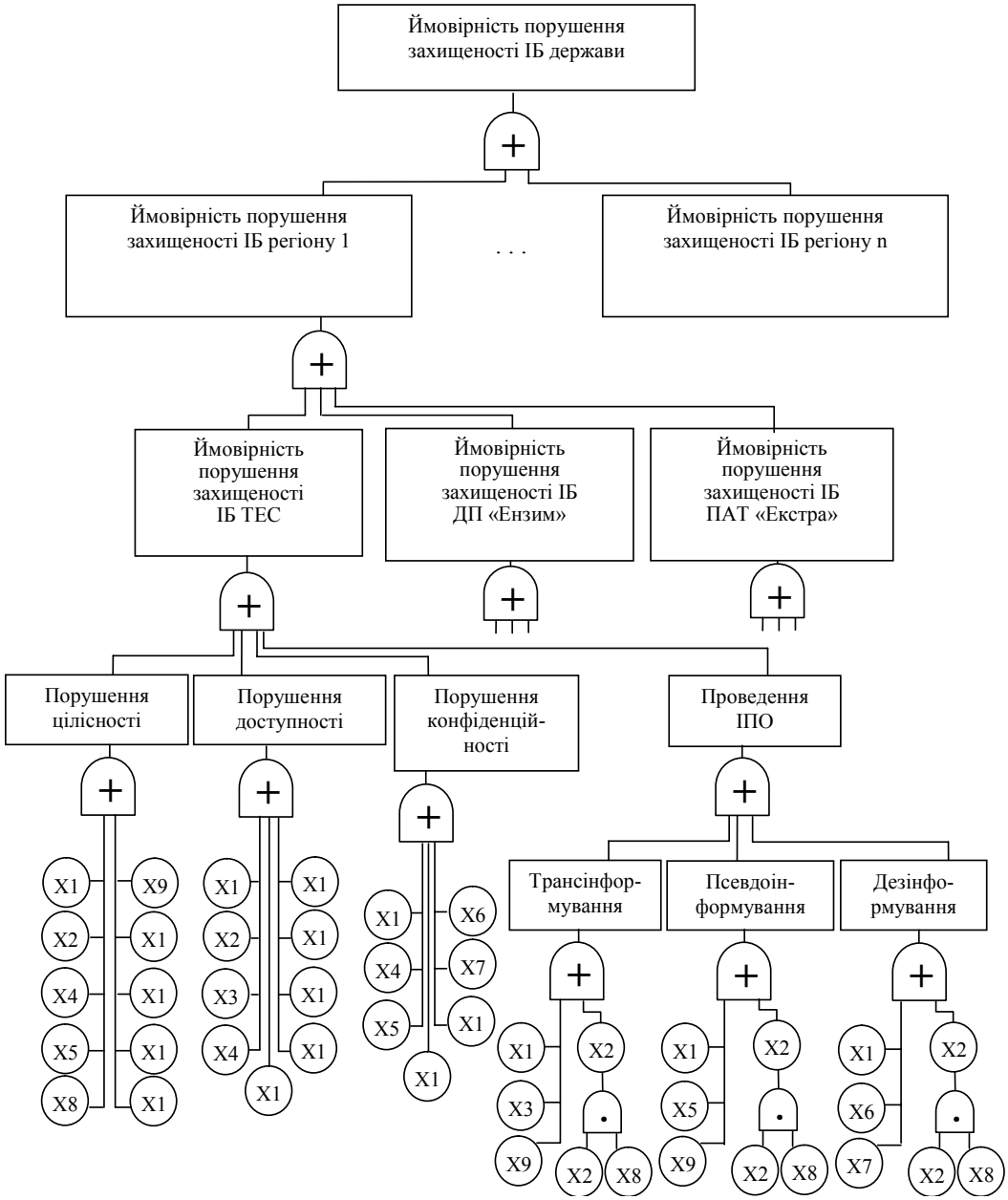

Рисунок 2 – Логіко-ймовірнісна модель оцінювання рівня комплексної інформаційної захищеності держави

Наведений фрагмент логіко-ймовірнісної моделі демонструє інтегрованість моделі формалізованої виразом (4). На базовому рівні представлено загрози, які існують на рівні відповідного об'єкта захисту. Проведення аналізу моделі передбачено у двох режимах: чіткому режимі, та нечіткому режимі. Чіткий режим, характеризується тим, що базові події визначаються ймовірностями, а нечіткий – експертними оцінками, які формалізуються нечіткими множинами.

Приклад аналізу подібних моделей наведений у [9, 10]. Нечіткі оцінки базових подій задано у LR-формі нечіткої множини. LR-форму нечіткого числа A можна представити у вигляді трійки значень $A = (m_A, \alpha_A, \beta_A)$. Для розрахунку ймовірностей виникнення можливих подій використано наступні арифметичні операції над нечіткими множинами, які можна визначити через операції над відповідними трійками:

$$A - B = (m_A, \alpha_A, \beta_A) - (m_B, \alpha_B, \beta_B) = \\ = (m_A - m_B, \alpha_A + \alpha_B, \beta_A + \beta_B), \quad (5)$$

$$A \times B = (m_A, \alpha_A, \beta_A) \cdot (m_B, \alpha_B, \beta_B) = \\ = (m_A \cdot m_B, m_A \cdot \alpha_B + m_B \cdot \alpha_A, m_A \cdot \beta_B + m_B \cdot \beta_A). \quad (6)$$

Якщо $\alpha = \beta = 0$, то нечітке число A переходе в чітке число m.

Розрахунки нечітких множин передбачає використання функцій належності за допомогою яких лінгвістична інформація може бути опрацьована. Для LR-форми не-

чіткої множини аналітичний вигляд функції належності представлено таким аналітичним виразом [11]:

$$\mu_A(\tilde{x}) = \begin{cases} 0, & a < \alpha_A, \\ \dfrac{a - \alpha_A}{m_A - \alpha_A}, & \alpha_A \le a < m_A, \\ \dfrac{\beta_A - a}{\beta_A - m_A}, & m_A < a \le \beta_A, \\ 0, & a > \beta_A. \end{cases} \quad (7)$$

Дефазифікація отриманих результатів виконується за допомогою методу центру ваг за формулою:

$$a = \frac{\sum_{i=1}^{n} \mu_A(\tilde{x}_i) \cdot \tilde{x}_i}{\sum_{i=1}^{n} \mu_A(\tilde{x}_i)}. \quad (8)$$

4 ЕКСПЕРИМЕНТИ

Для інформаційної підтримки щодо управління комплексною інформаційною безпекою розроблено програмне забезпечення, яке дозволяє автоматизувати процес аналізу рівня захищеності багаторівневої системи типу «підприємство – регіон – держава». Виконаємо експериментальне дослідження за допомогою розробленого програмного засобу, який реалізує запропоновані моделі.

Наведений нижче інтерфейс демонструє послідовність дій для виконання моделювання виконання ймовірних спеціальних інформаційних операцій. На рис. 3 представлено головне вікно програми, яке демонструє можливість вибору регіону. В даному випадку під регіоном розуміється кожна область України, хоча за необхідністю певні області можна об'єднувати і отримати, наприклад, Подільський регіон, регіон Полісся, тощо.

Наступним кроком після вибору регіону є вибір локальних об'єктів захисту або окремих підприємств. Вікно представлене на рис. 4 надає можливість побудови логіко-ймовірнісної моделі оцінювання рівня захищеності для окремого підприємства, а також вибору режиму розрахунку – чіткого або нечіткого.

На рис. 4. наведено приклад введення вхідних даних для аналізу окремого підприємства – Ладижинської ТЕС, яке розташовано у Вінницький області.

Отримані рівні захищеності окремих підприємств, які ототожнюються з ймовірностями несанкціонованого доступу до інформаційних ресурсів є вхідними даними для виконання аналізу рівня захищеності відповідного регіону. Аналогічні дії операції виконані для локальних об'єктів захисту, що розташовані у Львівському та Волинському регіонах.

Результати аналізу комплексної інформаційної безпеки на рівні держави, який в даному випадку включає 3 регіони, представлені Львівською, Волинською та Вінницькою областями, представлені на рівні рис. 5.

5 РЕЗУЛЬТАТИ

На рис. 4. наведено приклад введення вхідних даних для аналізу окремого підприємства – Ладижинської ТЕС, яке розташовано у Вінницький області. Крім того експертні оцінювання проводилися для підприємств ДП «Ензим» та ПАТ «Екстра».

Фрагмент експертних оцінок ймовірностей виникнення загроз поданих як нечіткі числа з трикутною функцією належності наведено в табл. 1.

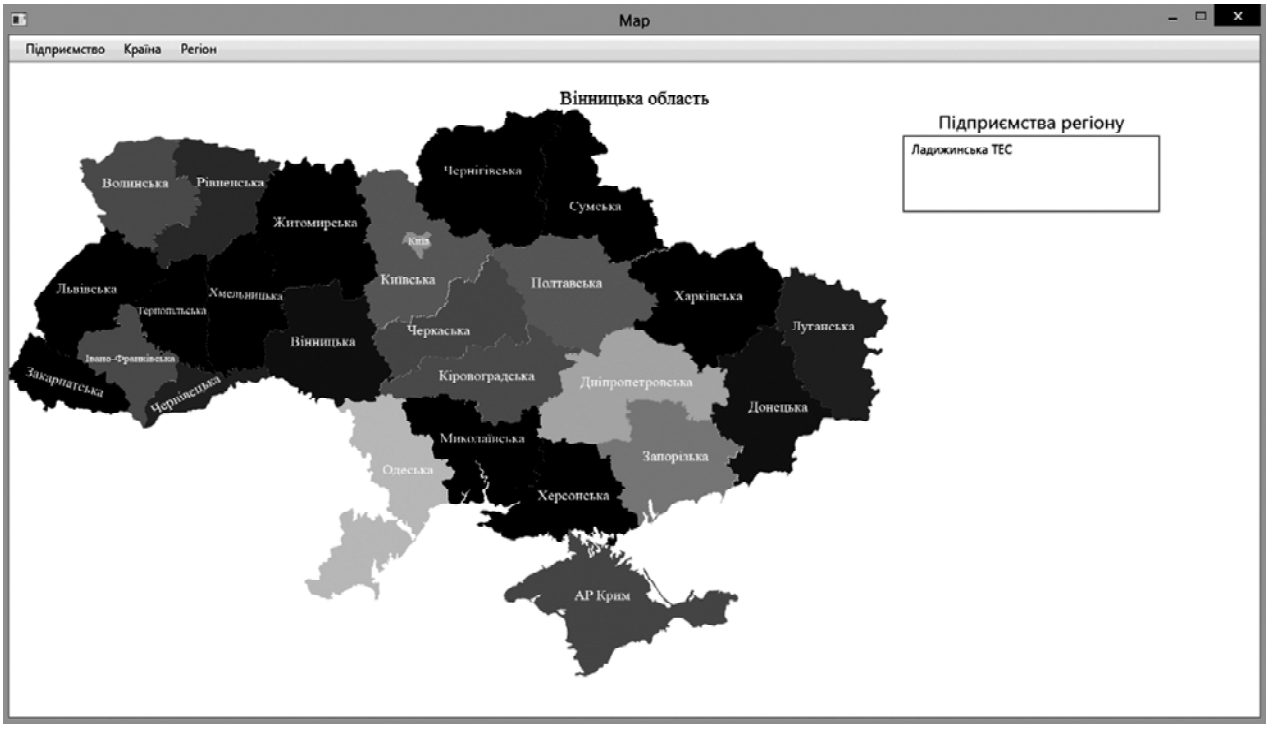

Рисунок 3 – Головне вікно програмного засобу для вибору регіону

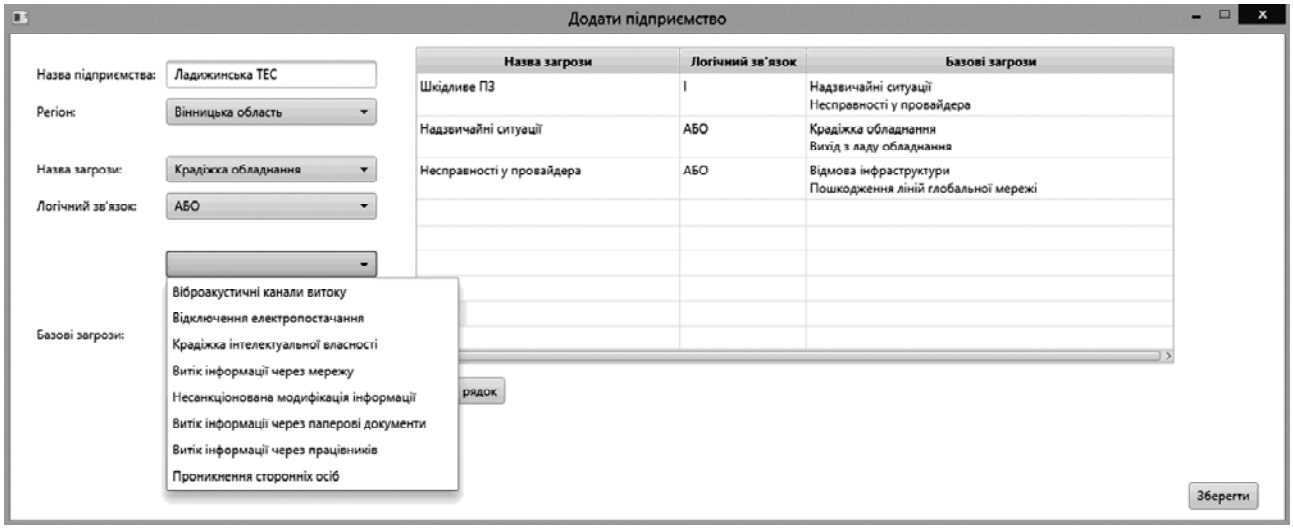

Рисунок 4 – Вікно для введення даних для аналізу окремого підприємства

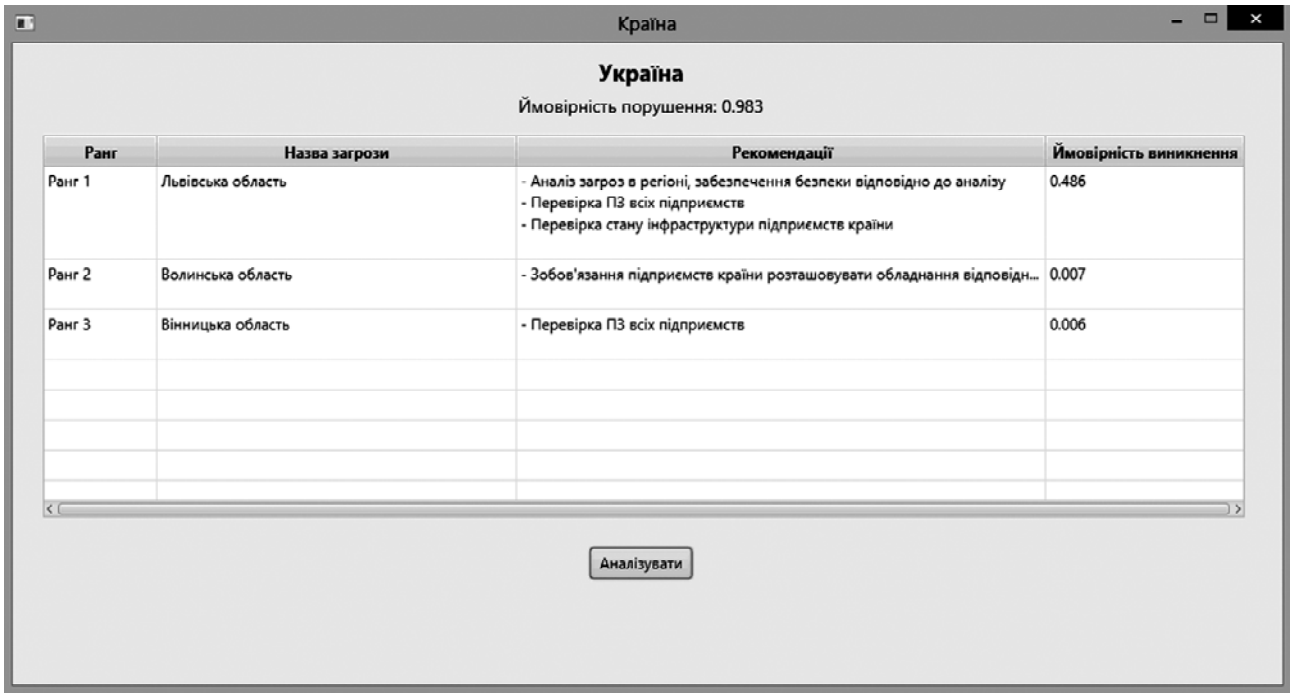

Рисунок 5 – Результати аналізу рівня захищеності на рівні держави

Таблиця 1 – Експертні оцінки ймовірностей виникнення загроз

Загроза		Ймовірність виникнення загрози		
		Лад. ТЕС	ДП «Ензим»	ПАТ «Екстра»
x_1	Порушення фізичної цілісності АС (її окремих компонентів), пристроїв, обладнання, носіїв інформації	{0,12; 0,02;0,03}	{0,13; 0,02;0,01}	{0,1; 0,02;0,03}
x_2	Модифікація інформаційних ресурсів, в тому числі програмного забезпечення	{0,09; 0,01;0,02}	{0,11; 0,01;0,02}	{0,12; 0,03;0,02}
x_3	Порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної, пожежної сигналізації тощо)	{0,08; 0,03;0,02}	{0,12; 0,03;0,02}	{0,1; 0,01;0,01}

Представлені експертні оцінки є вхідними даними для виконання аналізу рівня захищеності на рівні окремих підприємств. Результати аналізу представлені у табл. 2.

Оцінка порушення захищеності інформаційної безпеки Вінницького регіону:

$$P = (0{,}99;\ 1{,}25\cdot10^{-11};\ 1{,}22\cdot10^{-11}).$$

Аналіз отриманих даних показав, що ймовірність порушення захищеності інформаційної безпеки районного рівня становить 99,98%, з відхиленням зліва на $1{,}25\cdot10^{-9}$ та справа на $1{,}22\cdot10^{-9}$.

Висока ймовірність порушення захисту інформаційних ресурсів регіону пояснюється суб'єктивними експертними оцінками, а також врахуванням можливістю проведення ІПО проти соціальної частини СТС, як на рівні окремого підприємства, так і на рівні регіону та держави.

Таблиця 2 – Оцінки порушення комплексної інформаційної безпеки підприємств

Підприємство	Оцінка порушення цілісності	Оцінка порушення доступності	Оцінка порушення конфіденційності	Оцінка проведення ІПО	Оцінка порушення захищеності ІБ
Ладижинська ТЕС:	(0,940; $1{,}4\cdot10^{-2}$; $1{,}3\cdot10^{-2}$)	(0,882; $2{,}86\cdot10^{-2}$; $2{,}7\cdot10^{-2}$)	(0,813; $3{,}5\cdot10^{-2}$; $3{,}3\cdot10^{-2}$)	(0,883; $3{,}81\cdot10^{-2}$; $3{,}14\cdot10^{-2}$)	(0,9998; $1{,}5\cdot10^{-4}$; $1{,}4\cdot10^{-4}$)
ДП «Ензим»:	(0,945; $1{,}49\cdot10^{-2}$; $1{,}41\cdot10^{-2}$)	(0,881; $2{,}92\cdot10^{-2}$; $2{,}64\cdot10^{-2}$)	(0,816; $3{,}12\cdot10^{-2}$; $3{,}13\cdot10^{-2}$)	(0,871; $3{,}33\cdot10^{-2}$; $3{,}44\cdot10^{-2}$)	(0,9998; $1{,}4\cdot10^{-4}$; $1{,}4\cdot10^{-4}$)
ПАТ «Екстра»:	(0,945; $1{,}49\cdot10^{-2}$; $1{,}41\cdot10^{-2}$)	(0,871; $3{,}07\cdot10^{-2}$; $2{,}76\cdot10^{-2}$)	(0,784; $3{,}13\cdot10^{-2}$; $3{,}23\cdot10^{-2}$)	(0,886; $2{,}38\cdot10^{-2}$; $3{,}37\cdot10^{-2}$)	(0,9998; $1{,}7\cdot10^{-4}$; $1{,}8\cdot10^{-4}$)

Перспективи подальших досліджень полягають у формуванні на бази інцидентів, пов'язаних з проведенням ІПО та ІКО, бази знань державного, регіонального та локального рівнів та практичної реалізації запропонованого підходу до побудови ІАЦ управління комплексною інформаційною безпекою.

6 ОБГОВОРЕННЯ

Запропонована математична модель інформаційної підтримки управління комплексною інформаційною безпекою дозволяє враховувати кількісні оцінки ймовірностей виникнення загроз, а також експертні оцінки, що формалізовані у вигляді нечітких множин.

Результати моделювання показали, що запропонована модель, порівняно із існуючими, дозволяє отримати оцінку рівня захищеності як на рівні локального об'єкту захисту – підприємства, так і на рівнях інтегрованих об'єктів захисту – регіону та держави.

Представлені узагальнена математична модель для оцінювання рівня інформаційної захищеності багаторівневої системи, структурна модель багаторівневого ІАЦ, а також спеціальне програмне забезпечення, дозволять вирішити актуальну задачу щодо інформаційної підтримки управління комплексною інформаційною безпекою, відповідно до ISO/IEC 27001:2013 та НДТЗІ 1.4-001-2000.

ВИСНОВКИ

У роботі вирішено актуальну задачу розробки моделі та структури інформаційно-аналітичних центрів інформаційної підтримки прийняття рішень управління комплексною інформаційною безпекою багаторівневою СТС.

Наукова новизна роботи полягає в тому, що вперше запропоновано модель оцінювання комплексної інформаційної безпеки багаторівневої СТС на рівнях управління «підприємство – регіон – держава», яка на відміну від існуючих дозволяє отримати оцінку як локального об'єкта захист – підприємства, так і інтегрованих об'єктів захисту – регіону та держави з урахуванням ризиків ведення інформаційної війни, що дозволить реалізувати прийняття адекватних управлінських рішень.

Практична новизна полягає у розробці програмного забезпечення, яке реалізує процес аналізу та оцінювання рівня комплексної інформаційної захищеності багаторівневої СТС на рівнях управління «підприємство – регіон – держава», а також синтезу управлінських рішень на базі сформованих баз знань. Отримані бази знань дозволяють також організувати навчання управлінського персоналу.

ПОДЯКИ

Роботу виконано в рамках держбюджетної науково-дослідної теми Вінницького національного технічного університету «Методологія комплексного захисту інформації в соціотехнічних системах в умовах інформаційної війни» (номер державної реєстрації 0115U001125).

СПИСОК ЛІТЕРАТУРИ

1. Ситуационные центры в решении проблем информационной безопасности [Електронний ресурс] – Режим доступу до ресурсу: http://www.itsec.ru/articles2/Inf_security/sit_cents [Назва з екрану].
2. Президент ввів у дію рішення РНБО про Головний ситуаційний центр [Електронний ресурс] – Режим доступу до ресурсу: http://www.ukrinform.ua/rubric-iac/1820573-poroshenko_vviv_u_diyu [Назва з екрану].
3. Корченко А. Г. Системы анализа и оценивания рисков информационной безопасности: монография / А. Г. Корченко, А. Е. Архипов, С. В. Казмирчук. – Издательский Дом Palmarium Academic Publishing, 2013. – 316 с.
4. Ильин Н. И. Ситуационные центры. Опыт, состояние, тенденции развития / Н. И. Ильин, Н. Н. Демидов, Е. В. Новикова. – М. : Медиа Пресс, 2011. – 336 с.
5. Simola J. Common Cyber Situational Awareness: An Important Part of Modern Public Protection and Disaster Relief / J. Simola, J. Rajamäki // Proceedings of the 10th International Conference on Computer Engineering and Applications (CEA\'16), Barcelona. – 2016.
6. A streaming-based network monitoring and threat detection system / [Z. Chen, H. Zhang, W. Hatcher, etc]. // Software Engineering Research Management and Applications (SERA) 2016 IEEE 14th International Conference on. – 2016. – С. 31–37.
7. A cloud computing based architecture for cyber security situation awareness / [YU, Wei, et al.]. // Communications and Network Security (CNS), 2013 IEEE Conference on. IEEE. – 2013. – P. 488–492.
8. Рябинин И. А. Надежность и безопасность структурно-сложных систем / И. А. Рябинин. – СПб.: Политехника, 2000. – 248 с.
9. Дудатьєв А. В. Розробка уніфікованих моделей системного проектування оптимальних систем захисту інформаційних ресурсів / А. В. Дудатьєв // Вісник Черкаського технологічного університету. – 2008. – № 1. – С. 3–8.
10. Дудатьев А. В. Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны / А. В. Дудатьєв, В. А Лужецкий, Д. А. Коротаев // Восточно-Европейский журнал передовых технологий. – 2016. – № 1. – С. 4–11.
11. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети / А. П. Ротштейн. – Винница : УНИВЕРСУМ – Винница, 1999. – 320 с.

Стаття надійшла до редакції 18.11.2016.
Після доробки 21.12.2016.

Дудатьев А. В.[1], Войтович О. П.[2]

[1]Канд. техн. наук, доцент, доцент кафедры защиты информации Винницкого Национального Технического Университета, Винница, Украина

[2]Канд. техн. наук, доцент, доцент кафедры защиты информации Винницкого Национального Технического Университета, Винница, Украина

МОДЕЛИ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ УПРАВЛЕНИЯ КОМПЛЕКСНОЙ ИНФОРМАЦИЙОНОЮ БЕЗОПАСНОСТЬЮ

Актуальность. Существование конкурентной информационной среды, которая является специфической ареной для проведения специальных информационных операций, показывает необходимость реализации комплексной защиты информационных ресурсов. Ход информационной войны и проблемы, возникающие при управлении комплексной информационной безопасностью, определяет актуальность разработки моделей информационной поддержки принятия решений, а также создания ситуационных или информационно-аналитических центров управления комплексной информационной безопасностью на уровне «предприятие – регион – государство».

Цель. Целью данного исследования является разработка модели информационной поддержки принятия решений управления комплексной информационной безопасностью многоуровневой социотехнической системой в составе отдельных объектов, групп объектов (региона) и государства в целом, что позволит получить количественные показатели уровня защищенности системы с возможностью принятия решений по управлению комплексной информационной безопасностью на уровнях «предприятие – регион – государство».

Метод. Метод исследования строится на идее того, что уровень защищенности государства зависит от уровня защищенности подчиненных регионов, уровень защищенности которых, в свою очередь, зависит от уровня защищенности подчиненных локальных объектов. Уровень защищенности самого предприятия зависит от нарушения хотя бы одного из критериев: целостности, доступности, конфиденциальности.

Результаты. Решена задача разработки обобщенной модели оценки комплексной информационной безопасности многоуровневой социотехнической системы типа «предприятие – регион – государство», что позволяет получить оценку уровня информационной защищенности, как локального объекта – предприятия, так и интегрированных объектов – региона и государства. Для оценки вероятностей возникновения базовых угроз могут быть использованы вероятностные или экспертные оценки, представленные в виде нечетких множеств. Предложена структурная модель многоуровневого информационно-аналитического центра управления комплексной информационной безопасностью. Результаты проведенных исследований показали возможность использования данного подхода для решения задач оценки и управления комплексной информационной безопасностью многоуровневой социотехнической системы.

Выводы. Научная новизна проведенного исследования заключается в том, что впервые предложена модель оценки комплексной информационной безопасности многоуровневой социотехнической системы на уровнях управления «предприятие – регион – государство».

Практическая ценность заключается в разработке программного обеспечения, реализующего процесс анализа и оценки уровня комплексной информационной защищенности многоуровневой социотехнической системы на уровнях управления «предприятие – регион – государство», а также синтеза управленческих решений на базе сформированных баз знаний.

Ключевые слова: социотехническая система, комплексная информационная безопасность, информационная война, специальные информационные операции, информационно-аналитический центр, поддержка принятия решений.

Dudatyev A. V.[1], Voitovych O. P.[2]

[1]PhD, Associate Professor, Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia, Ukraine

[2]PhD, Associate Professor, Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia, Ukraine

MODELS OF INFOMATIONAL DECISION SUPPORT FOR THE COMPLEX INFORMATION SECURITY MANAGMENT

Context. The existence of a competitive information environment, which is a specific arena for special information operations, shows the necessity for implemention of information resources complex protection. Information warfare and the problems, those arise in the field of complex information security management, determine the relevance of the information decision support models development, as well as the creation of situational or information-analytical centers of the complex information security at the «Enterprise – Region – State» management levels.

Objective. The goal of this research is a development of information decision support model of the complex information security management of the multi-level socio-technical system which is consists of the individual objects, groups of objects (region) and the State en block, which would provide security level quantitative indicators as well as the ability to make decisions for the complex information security at the «Enterprise – Region – State» levels management.

Method. The method of this research is based on the idea that the State protection level depends on the subordinate regions protection level, which in its turn, depends on the subordinate local objects (enterprise) protection level. The enterprise protection level depends on the violation of at least one of the criteria: integrity, availability, confidentiality.

Results. The task of developing of the generalized model for complex information security of the multi-level socio-technical system evaluation in terms of «Enterprise – Region – State» is solved, which allows obtaining an protection level estimation of the both local (enterprise) and integrated (region and the State) objects. The probabilistic or expert evaluations in the form of fuzzy sets can be used for base threat occurrence estimation. The structural model of multi-level information-analytic center of the complex information security management is proposed. The results of researching have shown the possibility of using this approach for estimation and management problem solution of information security management for complex information security of the multi-level socio-technical systems.

Conclusions. Scientific novelty of the research is in the fact that the complex information security at the «Enterprise – Region – State» management levels evaluation model is proposed for the first time.

Practical significance consists in the development of the software implemented the process of complex information security of the multi-level socio-technical systems evaluation in terms of «Enterprise – Region – State» analyzing and estimation, as well as the synthesis of management decisions based on the generated knowledge bases.

Keywords: sociotechnical system, complex information security, information warfare, special informational operations, informational-analytic center, decision support.

REFERENCES

1. Situational centers in addressing issues of information security. Available on : http://www.itsec.ru/articles2/Inf_security/sit_cents.
2. President enacted the National Security Council decision on the main situational center. Available on : http://www.ukrinform.ua/rubric-iac/1820573-poroshenko_vviv_u_diyu_
3. Korchenko A. G., Arkhipov A. Ye., Kazmirchuk S. V. Sistemy analiza i otsenivaniya riskov informatsionnoy bezopasnosti: monografiya. Izdatelskiy Dom Palmarium Academic Publishing, 2013, 316 p.
4. Ilin N.I., Demidov N. N., Novikova Ye. V. Situatsionnye tsentry. Opyt, sostoyanie, tendentsii razvitiya. Moscow, MediaPress, 2011, 336 p.
5. Simola J., Rajamäki J. Common Cyber Situational Awareness: An Important Part of Modern Public Protection and Disaster Relief, *Proceedings of the 10th International Conference on Computer Engineering and Applications (CEA\'16)*. Barcelona, 2016.
6. Chen Z., Zhang H., Hatcher W., etc A streaming-based network monitoring and threat detection system, *Software Engineering Research Management and Applications (SERA) 2016 IEEE 14th International Conference on*, 2016, pp. 31–37.
7. YU, Wei, et al. A cloud computing based architecture for cyber security situation awareness, *Communications and Network Security (CNS), 2013 IEEE Conference on. IEEE*, 2013, pp. 488–492.
8. Ryabinin I. A. Nadezhnost i bezopasnost strukturno-slozhnykh sistem. Sankt-Peterburg, Politekhnika, 2000, 248 p.
9. Dudatyev A. V. Rozrobka unifikovanykh modelei systemnoho proektuvannia optymalnykh system zakhystu informatsiinykh resursiv, *Visnyk Cherkaskoho tekhnolohichnoho universytetu,* 2008, No. 1, pp. 3–8.
10. Dudatyev A. V., Luzhetskiy V. A., Korotaev D. A. Metod otsenki informatsionnoy ustoychivosti sotsiotekhnicheskikh sistem v usloviyakh informatsionnoy voyny, *Vostochno-Yevropeyskiy zhurnal peredovykh tekhnologiy*, 2016, No. 1, pp. 4–11.
11. Rotshteyn A. P. Intellektualnye tekhnologii identifikatsii: nechetkie mnozhestva, geneticheskie algoritmy, neyronnye seti. Vinnitsa, UNIVYERSUM-Vinnitsa, 1999, 320 p.