МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ
НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

VIII науково-практична конференція

Збірник матеріалів
(Київ, 24 травня 2017 року)

Електронна версія

Київ
2017

економічній сферах нашій державі доцільно розвивати наступні напрямки діяльності:

1) врегулювання національної нормативно-правової бази, яка б відповідала вимогам, що висуваються сучасним рівнем розвитку технологій; адаптація вітчизняного законодавства до правового поля провідних країн світу;

2) участь у міжнародних організаціях по боротьби з кіберзлочинністю, кібершпигунством;

3) якісна підготовка та забезпечення висококваліфікованими фахівцями підрозділів по боротьби з кіберзлочинністю в правоохоронних органах України;

4) підвищення рівня кваліфікації користувачів інформаційно-телекомункаційних систем, в яких циркулює інформація з обмеженим доступом;

5) організація взаємодії і координація зусиль правоохоронних органів та військових формувань, судової системи, забезпечення їх необхідною матеріально-технічною базою;

6) удосконалення технічного захисту інформації з обмеженим доступом в інформаційно-телекомункаційних системах, розголошення якої загрожує національній безпеці та обороні країни; розробка (модернізація) та виробництво на державних підприємствах сучасних спеціальних технічних та програмних засобів з технічного захисту інформації.

УДК 354.42

Небава М.І.
кандидат економічних наук, професор,
Вінницький національний технічний університет
Міронова Ю.В.
кандидат економічних наук,
Вінницький національний технічний університет

ІНТЕГРАЛЬНИЙ ПІДХІД ДО ОЦІНЮВАННЯ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Сучасні глобалізаційні та динамічні процеси розвитку цивілізації, посилення зовнішньої інформаційної агресії, а також жорстка конкуренція у контексті євроінтеграції вимагають забезпечення від служб безпеки посиленої охорони інформаційного простору [1]. Також визначальним є організація режиму безпеки та здійснення всіх видів діяльності, які забезпечують інформаційну та кібербезпеку.

Мета дослідження полягає у розробці інтегрального методично-

го підходу до оцінювання рівня захисту інформаційного простору, що уможливить покращення якості управлінського процесу.

Рівень інформаційної безпеки залежить від спроможності уникати загроз і ліквідовувати шкідливі наслідки окремих негативних складових зовнішнього і внутрішнього середовища [2]. Ефективним управлінським рішенням передує глибокий аналіз та оцінка предмету дослідження [3]. Отже, необхідною задачею для кожного управлінського апарату є оцінювання рівня власної безпеки. Процес оцінювання безпеки представляє собою систему реалізації ряду функцій. Задача полягає у знаходженні ряду показників та функцій перетворення, на основі яких буде складена система оцінки.

Основна проблема оцінки безпеки полягає у тому, що її неможливо оцінити, враховуючи вузьке коло початкових показників, або на основі єдиного показника. Оцінка має відображати усі сторони загроз і ризиків для суб'єкта. Також вхідні показники мають бути зрозумілими та доступними для відображення у моделі.

Враховуючи представлені критерії було розроблено алгоритм оцінювання безпеки інформаційного простору (рис 1).

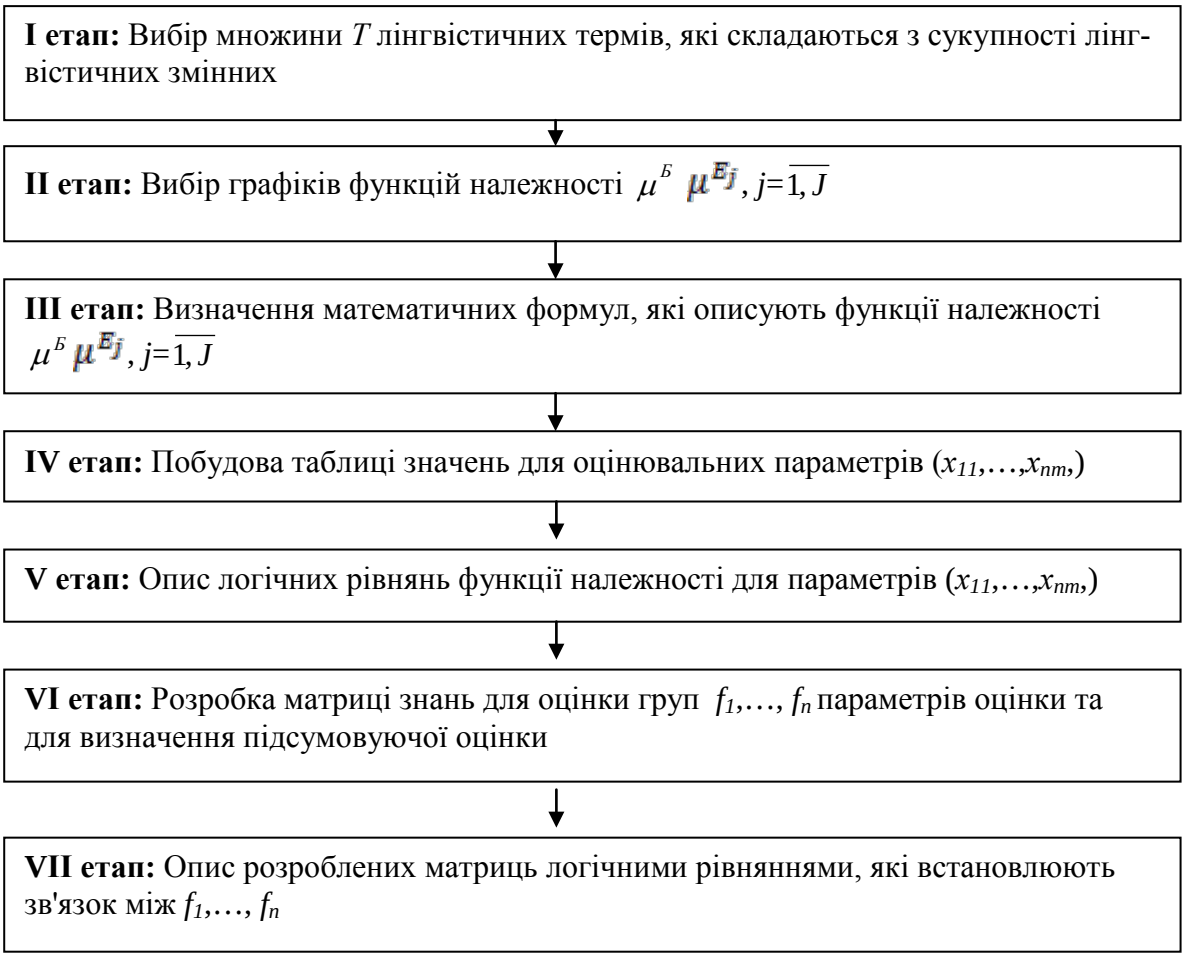

Рисунок 1 − Етапи оцінювання безпеки інформаційного простору
Джерело: авторська розробка

Згідно представленої схеми, початком процесу є вибір лінгвістичних термів, які будуть відображати рівень безпеки. Далі, використовуючи математичний апарат нечітких множин [4, 5], було складено графіки функції належності, визначено математичні формули опису функції належності. Відбір показників здійснено на основі критеріїв повноти, дієвості та мінімальності. Наступним етапом є формування матриць знань для обраних показників – здійснюється на основі методу експертних оцінок. Розроблені матриці описуються логічними рівняннями, на основі яких і отримується остаточне значення або характеристика рівня безпеки.

Отже, розроблений інтегральний методичний підхід на базі математичного апарату нечітких множин дає змогу оцінити рівень безпеки інформаційного простору, враховуючи технологічну, ресурсну, фінансову та соціальну безпеку [6]. Головна особливість розробленої моделі – обчислювальна ефективність і гарантованість результатів.

Література

1. Небава М. І. Глобалізаційні процеси та головні виклики для національного середовища України / М. І. Небава, В. О. Денисенко // Materials of the XI International scientific and practical conference, «Modern European scienze», – 2015. Volume 3. Economic science. Covernance. Political science. 2015. – С.60-61.

2. Архірейська Н. В. Економічна безпека в контексті державної стратегії України / Н. В. Архірейська // Сучасні тенденції розвитку фінансових та інноваційно-інвестиційних процесів в Україні: Матеріали міжнародної науково-практичної конференції. – Вінниця: ВНТУ, 2013. – С. 8−10.

3. Бойченко О. В. Політика інформаційної безпеки в системі інформаційного забезпечення ОВС України / О. В. Бойченко // Форум права. – 2009. – № 1. – С. 50–55.

4. Заде Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений. Москва: Мир,1976. – 167 с.

5. Ротштейн А. П. Інтелектуальні технології ідентифікації: нечіткі множини, генетичні алгоритми, нейронні мережі. Монографія / А. П. Ротштейн. – 1999. – 320 с.

6. Небава М. І. Забезпечення енергетичної, економічної та екологічної безпеки України в контексті сталого розвитку / М. І. Небава, О. В. Стрелюк // V-ий Всеукраїнський з'їзд екологів з міжнародною участю (Екологія / Ecology -2015), 23-26 вересня 2015. Збірник наукових праць. – Вінниця: ТОВ «Нілан ЛТД», 2015. – С. 277.