МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ГОЛОЛОБОВ Андрій Юрійович

УДК 004.056.5(043)

МЕТОДИ ТА МОДЕЛІ АДАПТИВНИХ СИСТЕМ ОЦІНКИ РИЗИКІВ

05.13.21 – системи захисту інформації

Автореферат

дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2017

Дисертацією є рукопис.

Робота виконана в Національному авіаційному університеті Міністерства освіти і науки України

Науковий керівник: кандидат технічних наук, доцент
Казмірчук Світлана Володимирівна,
Національний авіаційний університет,
доцент кафедри безпеки інформаційних технологій.

Офіційні опоненти: доктор технічних наук, старший науковий співробітник
Грищук Руслан Валентинович,
науковий центр Житомирського військового інституту ім. С.П. Корольова, начальник відділу інформаційної та кібернетичної безпеки;

кандидат технічних наук,
Цуркан Василь Васильович
Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ ім. Ігоря Сікорського», провідний науковий співробітник.

Захист відбудеться «13» квітня 2017 р. о 14.00 годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, Київ, пр. Космонавта Комарова, 1.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «11» березня 2017 р.

В.о. ученого секретаря
спеціалізованої вченої ради В.П. Квасніков

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Поширення інформаційних технологій (ІТ) в усі сфери життєдіяльності людини та суспільства стало нормою сучасної цивілізації та сприяє її подальшій еволюції. Стрімкий розвиток і розповсюдження нових інформаційно-комунікаційних технологій набуває сьогодні характеру безпрецедентної за своїми масштабами інформаційної революції, яка стає вирішальним фактором розвитку людства. Збільшення ролі інформації у житті суспільства, створення глобального інформаційного простору, який забезпечує ефективну комунікативну взаємодію людей, їхній доступ до світових інформаційних ресурсів і задоволення соціальних та особистісних потреб в інформаційних продуктах і послугах, є реаліями сьогодення. Інформація перетворюється в основне джерело інтенсифікації і гармонізації суспільного розвитку, тому перед суспільством стає проблема швидкого оволодіння інформацією, способів її осмислення та оцінки, механізмів ефективного використання, забезпечення інформаційної безпеки (ІБ). Розвиток ІТ-інфраструктури підприємства тягне за собою стрімке неконтрольоване збільшення вразливості ресурсів інформаційних систем (РІС).

У зв'язку з реальністю численних загроз і зростанням ролі РІС в житті сучасного суспільства, проблема ІБ вимагає до себе постійної і все більш зростаючої уваги. Системний характер впливу на ІБ великої сукупності різних обставин, які мають до того ж різну фізичну природу і викликають різноманітні наслідки, призводять до необхідності комплексного підходу при вирішенні даної проблеми. Отже, проблема ІБ складна, багатогранна і пов'язана з рішенням широкого спектру завдань, орієнтованих як на забезпечення надійності, так і на побудову моделей і систем оцінки її стану. Для забезпечення необхідного рівня безпеки РІС зазвичай на підприємствах впроваджують відповідні системи захисту інформації (ЗІ). Одним з основних етапів побудови таких систем є реалізація процесу аналізу і оцінювання ризиків (ОР) інформаційної безпеки, який дозволяє визначити необхідний рівень ЗІ, здійснити його підтримку і розробити стратегію розвитку інформаційної структури об'єкту захисту. Тому розробкою методів і засобів ОР активно займаються дослідники багатьох країн світу.

Розробками, пов’язаними з ОР у сфері ІБ, займались такі вітчизняні та закордонні учені, як О.Є. Архіпов, О.О. Замула, О.Г. Корченко, І.К. Совтус, В.П. Буянов, Я.Д. Вишняков, П.В. Грабовий, В.І. Завгородній, І.С. Медведовський, С.О. Петренко, А. Сайлім, С.В. Сімонов, Р.П. Томас, Є. Хорі, та ін.

Однак у сфері управління ризиками ІБ залишилось чимало завдань і проблем, які мають важливе наукове і практичне значення і потребують свого вирішення, зокрема, це стосується практичного ОР безпеки РІС в нечітких і детермінованих умовах з використанням параметрів, які можуть бути представлені, як в числовій, так і в лінгвістичній формі, із застосуванням експертних оцінок, що формуються в слабоформалізованому середовищу. Тому розробка нових і удосконалення існуючих методів оцінювання ризиків безпеки ресурсів інформаційних систем *є актуальною науковою задачею.*

Зв’язок роботи з науковими програмами, планами, темами. Результати дисертаційного дослідження відображені у звітах про науково-дослідні роботи: Кіровоградського національного технічного університету «Розробка методів синтезу тестових моделей поведінки програмних об’єктів, підвищення оперативності передачі

та захисту інформації у телекомунікаційних системах» (державна реєстрація № 0115U003103) та Національного авіаційного університету «Методологія оцінювання ризиків безпеки ресурсів інформаційних систем» (реєстраційний номер 105/14.01.05).

Мета і задачі дослідження. Метою дисертаційної роботи є розробка методів та моделей оцінювання ризиків безпеки РІС, які дозволяють будувати гнучкі засоби оцінювання з адаптивними еталонами параметрів.

Для досягнення поставленої мети **необхідно вирішити такі основні задачі:**

− Проаналізувати сучасні методи оцінювання ризиків з метою визначення набору ідентифікуючих та оціночних компонентів, які використовуються для створення інструментарію, орієнтованого на вирішення відповідних завдань захисту інформації;

– Розробити удосконалену бістабільну інтегровану кортежну модель характеристик ризику (БІМ), яка дозволяє динамічно визначати набори величин в аналітичному та синтетичному кортежах і таким чином забезпечити гнучкість розроблюваних засобів оцінювання ризиків безпеки ресурсів інформаційних систем;

– Розробити методи декрементування та інкрементування порядку лінгвістичної змінної (ЛЗ), що дозволить забезпечити адаптивні властивості еталонів параметрів розроблюваних засобів оцінювання ризиків безпеки ресурсів інформаційних систем;

– Розробити інтегрований метод оцінювання ризиків безпеки ресурсів інформаційних систем, який дозволяє створювати гнучкі засоби оцінювання та використовувати в якості вхідних даних динамічно змінювані набори детермінованих і нечітко визначених оціночних параметрів;

– Розробити модель процесу синтезу систем оцінювання ризиків для формалізації процесів побудови відповідних програмних та програмно-апаратних обчислювальних засобів;

− Розробити структурно-функціональну модель системи оцінювання ризиків безпеки ресурсів інформаційних систем для створення відповідного програмного застосунку;

− На основі запропонованої структурно-функціональної моделі, розробити програмну систему та здійснити експериментальне дослідження відповідного програмного забезпечення (ПЗ) з метою верифікації розроблених методів та моделей.

Об'єкт дослідження – процес оцінювання ризиків безпеки ресурсів інформаційних систем.

Предмет дослідження – методи та моделі оцінювання ризиків безпеки ресурсів інформаційних систем.

Методи дослідження. Проведені дослідження базуються на сучасних методах теорії нечіткої логіки (розробка методу ОР), прийняття рішень, об'єктно-орієнтованого програмування (розробка ПЗ системи ОР безпеки РІС), імітаційного моделювання інформаційних процесів і структур (проведення моделювання різних умов і середовища стану інформаційної системи при проведенні експериментального дослідження), а також «м'яких» обчисленнях.

Наукова новизна одержаних результатів полягає в наступному:

– *вперше розроблено* базові методи інкрементування та декрементування порядку лінгвістичних змінних, які за рахунок використання аналітичних функцій зменшення і збільшення термів на один порядок, дозволяють реалізовувати

трансформування базових еталонів параметрів без залучення експертів відповідної предметної галузі;

− *удосконалена* кортежна модель, яка за рахунок множин інтегрованих характеристик ризиків, підмножин їх ідентифікуючих і оціночних компонентів, бістабільних відображень в аналітичному та синтетичному кортежах, дозволяє ефективно організовувати процес вибору відповідних існуючих інструментальних засобів і розробляти гнучкі та ефективні методи і системи оцінювання ризиків інформаційної безпеки;

− *удосконалено* метод оцінювання ризиків безпеки ресурсів інформаційних систем, який за рахунок інтеграції детермінованого і нечіткого підходу оцінювання, бістабільної інтегрованої кортежної моделі характеристик ризику, базових методів інкрементування та декрементування порядку лінгвістичних змінних, дозволяє оперувати одночасно чіткими і нечіткими величинами з варіативним числом терм-множин;

− *удосконалено* модель процесу синтезу систем оцінювання ризиків, яка за рахунок використання базових методів інкрементування і декрементування порядку лінгвістичних змінних, бістабільної інтегрованої кортежної моделі характеристик ризику та інтегрованого методу оцінювання, дозволяє формалізувати процес створення адаптивних інструментальних засобів з гнучкими можливостями щодо перетворення заданих множин оброблюваних величин при оцінюванні ризику безпеки ресурсів інформаційних систем;

− *удосконалено* структурно-функціональну модель інтегрованої адаптивної системи оцінювання ризиків безпеки ресурсів інформаційних систем, яка за рахунок підсистем формування вхідних даних та обробки даних, що реалізують запропоновані методи (інтегрований, інкрементування і декрементування), дозволяє формувати і перетворювати дані як в якісній, так і в кількісній інтерпретації з можливістю трансформування еталонів параметрів без залучення експертів відповідної області.

Практичне значення одержаних результатів

Отримані під час виконання дисертаційної роботи результати можуть бути використані для проведення оцінювання ризиків безпеки ресурсів інформаційних систем на основі лінгвістичних і цифрових даних під час розробки систем менеджменту інформаційної безпеки та комплексних систем захисту інформації. Практична цінність роботи полягає в наступному:

− розроблено алгоритмічне забезпечення для реалізації програмної системи оцінювання ризиків безпеки ресурсів інформаційних систем;

− реалізована прикладна програмна адаптивна система оцінювання ризиків безпеки ресурсів інформаційних систем, яка використовує і динамічно визначає різні набори оціночних компонентів, що забезпечує високу гнучкість, функціональність і зручність її використання, як в детермінованому, так і в нечіткому, слабоформалізованному середовищі без залучення експертів відповідної предметної області.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1, 3-6] – формування складових етапів методів декрементування порядку ЛЗ та їх експериментальне дослідження; [2] – реалізація та експериментальне дослідження етапів методу ОР безпеки РІС; [7] –

розробка базових компонентів, що характеризують множину можливих характеристик ризику; [8] – експериментальне дослідження етапів удосконаленої моделі процесу синтезу систем ОР; [9, 10, 13] – реалізація міжкомпонентних зв'язків відповідно до їх функціональних властивостей та експериментальне дослідження структурно-функціональної моделі інтегрованої адаптивної обчислювальної системи ОР безпеки РІС; [11, 12, 14, 15] – формування складових етапів методів інкрементування порядку ЛЗ та їх експериментальне дослідження. З робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються результати, отримані особисто здобувачем.

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідалися та обговорювалися на наступних конференціях: I Международная научно-техническая конференция «Проблемы информатизации» (Черкаси, 2013 р.), XI Міжнародна науково-технічна конференція «АВІА-2013» (Київ, 2013 р.), 18-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке» (Харків, 2014 р.), 6-та Всеукраїнська науково-практична конференція «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2014)» (с. Коблево, Миколаївської обл., 2014 р.), науково-практична конференція «Актуальні питання забезпечення кібернетичної безпеки та захист інформації» (Київ, 2015 р.), міжвідомчий міжрегіональний семінар Наукової Ради НАН України «Технічні засоби захисту інформації» (Київ, 2013 р.).

Публікації. Основні положення дисертації опубліковано у 15 наукових працях, у тому числі 9 статей у наукових журналах та збірниках наукових праць, які входять до переліку наукових фахових видань України, 8 з яких опубліковані у рецензованих виданнях, що входять до міжнародних наукометричних баз даних та 6 тез доповідей і матеріалів конференцій.

Структура та об'єм дисертації. Дисертація складається зі вступу, чотирьох розділів, загальних висновків, додатку, списку використаних джерел і має 154 сторінки основного тексту, 33 рисунки, 37 таблиць. Список літератури містить 121 найменування і займає 14 сторінок. Додаток займає 3 сторінки. Загальний обсяг роботи 182 сторінки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** представлена загальна характеристика дисертаційної роботи, обґрунтована актуальність теми, сформульовано мету і завдання досліджень, відзначено наукову новизну та практичне значення одержаних результатів, визначено особистий внесок здобувача, наведено відомості про апробацію результатів роботи, публікації, структуру та об'єм дисертації.

Перший розділ присвячений огляду вітчизняної та зарубіжної літератури за темою дисертаційної роботи. Розглянуто використання в області інформаційної безпеки таких понять, як інформація, ризик, аналіз і оцінка ризиків. Детально розглянута модель інтегрованого представлення параметрів ризиків інформаційної безпеки, в якій ризики подано у вигляді десятикомпонентного кортежу, компоненти якого визначені, як: $\boldsymbol{E}$ – подія, $\boldsymbol{A}$ – дія, $\boldsymbol{M}$ – міра ризику, $\boldsymbol{C}$ – характеристика ситуації, $\boldsymbol{P}$ – імовірність, $\boldsymbol{D}$ – небезпека, $\boldsymbol{S}$ – ситуація вибору, $\boldsymbol{F}$ – частота, $\boldsymbol{L}$ – витрати і втрати (витрати), $\boldsymbol{V}$ – відхилення від мети. Проаналізовано сучасні методи оцінювання ризиків ІБ, зокрема, такі, як CRAMM, RiskWatch, COBRA, Гриф 2006, МБМ (метод на основі байєсових мереж). Особливу увагу приділено детермінованому методу

оцінювання ризиків ІБ, заснованому на бінарних оцінках, і нечіткому методу. За результатами аналізу визначено, що в основному для ОР використовуються статистичні дані про інциденти та загрози ІБ, а також наявність певних обмежень на використовуваний набір параметрів ризиків. У табл. 1 наведено дані щодо характеристик ризику, які використовуються в різних засобах ОР, де «+» відповідно вказують на наявність характеристики, а «–» його відсутність.

Таблиця 1

Зведені дані аналізу засобів ОР

Засоби ОР	Характеристики ризику					
	AES	CS/ D	E	F /L	M /P	V/A
COBRA	–	+/–	+	–/–	+/+	+
CRAMM	–	+/–	+	+/+	+/+	+
RiskWatch	–	+/–	+	+/+	+/+	+
RA2 art of risk	–	+/+	+	–/–	+/+	+
КЭС	–	+/+	+	–/+	+/+	+
Risk Advisor	–	+/+	+	–/+	+/+	+
vsRisk	–	+/+	+	–/–	+/+	+
OCTAVE	–	+/+	+	–/–	+/–	+
Гриф 2006	–	+/+	+	–/+	+/+	+
@RISK	–	+/–	+	–/+	+/+	+
RiskPAC	–	+/+	+	–/+	+/+	+
MSAT	–	+/+	+	–/–	+/–	+
МБМ	–	+/+	+	–/+	+/+	+
NIST 800-30	–	+/+	+	–/–	+/+	+
VAR	–	+/+	+	–/+	+/+	+
TRA	–	+/+	+	–/–	+/+	+
FRAP	–	+/–	+	–/+	+/+	+
BSI-Standard 100-3	–	+/–	+	–/–	+/–	+
ИББС-2.2-2009	–	+/+	+	+/+	+/+	+
ISO/IEC 27005	–	+/+	+	–/–	+/+	+
Risk Matrix	–	+/+	+	+/–	+/+	+
AS/NZS 4360:2004	–	+/+	+	–/–	+/+	+
Mehari	–	+/+	+	–/–	+/–	+
ISO/FDIS 31000	–	+/+	+	–/–	+/+	+
MAGERIT	–	+/+	+	+/+	+/+	+
Information SRA	–	+/+	+	–/–	+/+	+

Показана актуальність подальшого вдосконалення методів ОР ІБ, зокрема, створення методу, що використовує лінгвістичні змінні і дозволяє оперувати одночасно чіткими і нечіткими параметрами з вибором необхідної кількості терм-множин.

Другий розділ присвячений розробці моделі БІМ та базових методів для побудови адаптивних систем оцінювання ризиків інформаційної безпеки. Пропонується для інтегрованого представлення характеристик ризиків у сфері ІБ, відображати його у вигляді бістабільних відображень в аналітичному та синтетичному кортежах з урахуванням необхідної множини початкових компонентів. З метою формалізації процесу формування необхідних характеристик ризику пропонується так звана БІМ, структурно-аналітичне відображення якої представлено на рис. 1.

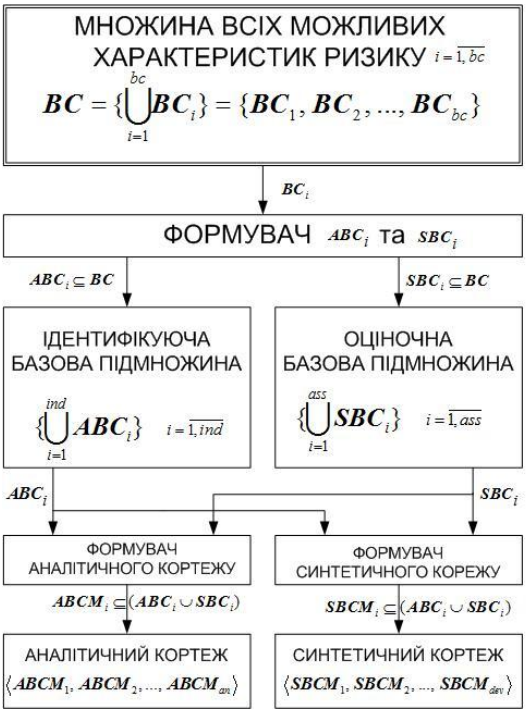

Рисунок 1 – Структурно-аналітичне відображення
бістабільної інтегрованої кортежної моделі характеристик ризику

З її допомогою для досягнення мети досліджень здійснюється формування необхідних аналітичного і синтетичного кортежів. Для цього введемо множину всіх можливих характеристик ризику:

$$\boldsymbol{BC}=\{\bigcup_{i=1}^{bc}\boldsymbol{BC}_i\}=\{\boldsymbol{BC}_1,\boldsymbol{BC}_2,...,\boldsymbol{BC}_{bc}\},\qquad(1)$$

де $\boldsymbol{BC}_i\subseteq\boldsymbol{BC}$ ($i=\overline{1,bc}$) – підмножина відображає *i*-ю характеристику ризику. Таку підмножину можемо представити, в наступному вигляді:

$$\boldsymbol{BC}_i=\{\bigcup_{bo=1}^{n_i}BC_{i,bo}\}=\{BC_{i,1},BC_{i,2},...,BC_{i,n_i}\}.\qquad(2)$$

Таким чином (1) з урахуванням (2) можемо записати як:

$$\{\bigcup_{i=1}^{bc}\boldsymbol{BC}_i\}=\{\bigcup_{i=1}^{bc}\{\bigcup_{bo=1}^{n_i}BC_{i,bo}\}\}=\{\bigcup_{i=1}^{bc}\{BC_{i,1},BC_{i,2},...,BC_{i,n_i}\}\}=$$
$$=\{\{BC_{1,1},BC_{1,2},...,BC_{1,n_1}\},\{BC_{2,1},BC_{2,2},...,BC_{2,n_2}\},...,\{BC_{bc,1},BC_{bc,2},...,BC_{bc,n_{bc}}\}\},\qquad(3)$$

де bc та n_i – відповідно кількість членів у $\boldsymbol{BC}$ і $\boldsymbol{BC}_i$, $(i=\overline{1,bc},\ bo=\overline{1,n_i})$.

В складі множини можуть бути наступні елементи:

Елемент ***AES*** – «Адаптивність нечітких шкал оцінювання» ($\boldsymbol{BC}_1$ = ***AES***), який може бути представлений у вигляді підмножини

$$\boldsymbol{BC}_1=\{\bigcup_{bo=1}^{n_1} BC_{1,bo}\}=\ \boldsymbol{AES}=\{\bigcup_{bo=1}^{aes} AES_{bo}\},$$

де ***AES*** – кількість варіантів адаптованості нечітких шкал оцінювання ($\boldsymbol{BC}_1\subseteq\boldsymbol{BC}$, $bo=\overline{1,aes}$), наприклад, при aes = 2

$$\boldsymbol{BC}_1=\{\bigcup_{bo=1}^{n_1} BC_{1,bo}\}=\{BC_{1,1},\ BC_{1,2}\}=$$

$$=\boldsymbol{AES}=\ \{\bigcup_{bo=1}^{2} AES_{bo}\}=\ \{AES_1,\ AES_2\}=\{\text{«декрементування», «інкрементування»}\},$$

($BC_{1,1}=AES_1$, $BC_{1,2}=AES_2$ – варіанти адаптованості нечітких шкал оцінювання для параметричних ***AES*** нечітких чисел (НЧ), наприклад, трапецієподібних і трикутних). Цей елемент відображає можливості системи щодо трансформування еталонів параметрів і адаптації системи під різні умови середовища оцінювання без участі експертів відповідної предметної області.

Елемент ***CA*** – «Калькулятор» ($\boldsymbol{BC}_2$ = ***CA***), який може відображатися у вигляді підмножини

$$\boldsymbol{BC}_2=\{\bigcup_{bo=1}^{n_2} BC_{2,bo}\}=\boldsymbol{CA}=\{\bigcup_{bo=1}^{ca} CA_{bo}\},$$

де ca – кількість варіантів калькулятора, ($\boldsymbol{BC}_2\subseteq\boldsymbol{BC}$, $bo=\overline{1,ca}$). Цей елемент показує наявність в системі можливості використання калькуляторів для оцінювання ризику, а також оцінок CVSS.

Елемент ***CS*** – «Характеристика ситуації» ($\boldsymbol{BC}_3$ = ***CS***), який можна визначити як підмножину

$$\boldsymbol{BC}_3=\ \{\bigcup_{bo=1}^{2} BC_{3,bo}\}=\ \{BC_{3,1},\ BC_{3,2}\}=$$

$$=\boldsymbol{CS}=\{\bigcup_{bo=1}^{2} CS_{bo}\}=\ \{CS_1,CS_2\}=\{\text{«Визначена», «Нечітка»}\},$$

де $BC_{3,1}=CS_1$, $BC_{3,2}=CS_2$ – елементи підмножини ***CS***, відображають характеристику ситуації у вигляді лінгвістичних значень.

Елемент ***D*** – «Небезпека» ($\boldsymbol{BC}_4$ = ***D***), який може відображатися за допомогою лінгвістичної змінної (ЛЗ)

$$\boldsymbol{BC}_4=\ \{\bigcup_{bo=1}^{n_4} BC_{4,bo}\}=\ \boldsymbol{D}=\{\bigcup_{bo=1}^{d} \underset{\sim}{D}_{bo}\},$$

де $n_4=d$ – кількість термів ЛЗ «НЕБЕЗПЕКА» ($\boldsymbol{BC}_4\subseteq\boldsymbol{BC}$, $bo=\overline{1,d}$).

Елемент ***DT*** – «Відхилення від мети» (***BC***$_5$ = ***DT***), який є характеристикою, що відображається у чисельному вигляді (наприклад, як стандартне (квадратичне), ймовірне або допустиме відхилення) або за допомогою застосування логіко-лінгвістичного підходу у вигляді ЛЗ «ВІДХИЛЕННЯ ВІД МЕТИ»,

$$\text{тобто} \quad \boldsymbol{BC}_5 = \{\bigcup_{bo=1}^{n_5} BC_{5,bo}\} = \boldsymbol{DT} = \{\bigcup_{bo=1}^{dt} \underset{\sim}{DT}_{bo}\},$$

де $n_5 = dt$ – кількість термів ЛЗ «ВІДХИЛЕННЯ ВІД МЕТИ»

$$(\boldsymbol{BC}_5 \subseteq \boldsymbol{BC}, \text{ а } \underset{\sim}{DT}_1 < \underset{\sim}{DT}_2 < ... < \underset{\sim}{DT}_{dt}, \quad bo = \overline{1, dt}).$$

Елемент ***E*** – «Порушення базових характеристик ІБ» (***BC***$_6$ = ***E***), який можна відобразити у вигляді символьної змінної, що приймає одне із значень кінцевої підмножини ідентифікаторів,

$$\boldsymbol{BC}_6 = \{\bigcup_{bo=1}^{n_6} BC_{6,bo}\} = \boldsymbol{E} = \{\bigcup_{bo=1}^{e} E_{bo}\},$$

де $n_6 = e$ – кількість ідентифікаторів порушення ІБ РІС ($\boldsymbol{BC}_6 \subseteq \boldsymbol{BC}, bo = \overline{1, e}$).

Елемент ***F*** – «Частота» (***BC***$_7$ = ***F***), який аналогічно ***D*** може визначатися ЛЗ «ЧАСТОТА», наприклад, при f =3 вона має вигляд:

$$\boldsymbol{BC}_7 = \{\bigcup_{bo=1}^{n_7} BC_{7,bo}\} = \{BC_{7,1}, BC_{7,2}, BC_{7,3}\} = \boldsymbol{F} = \{\bigcup_{bo=1}^{f} \underset{\sim}{F}_{bo}\} = \{\bigcup_{bo=1}^{3} \underset{\sim}{F}_{bo}\} = \{\underset{\sim}{F}_1, \ \underset{\sim}{F}_2, \ \underset{\sim}{F}_3\},$$

де $n_7 = f$ – кількість термів ЛЗ «ЧАСТОТА» ($\boldsymbol{BC}_7 \subseteq \boldsymbol{BC}$, $bo = \overline{1, f}$), а $BC_{7,1} = \underset{\sim}{F}_1$,

$BC_{7,2} = \underset{\sim}{F}_2$, $BC_{7,3} = \underset{\sim}{F}_3$ – елементи базової терм-множини $\boldsymbol{F}$, які відображають частоту у вигляді нечітких значень.

Елемент ***L*** – «Витрати» (***BC***$_8$ = ***L***), який може бути представлений у чисельному вигляді.

Елемент ***M*** – «Міра ризику» (***BC***$_9$ = ***M***), який можна представити підмножиною

$$\boldsymbol{BC}_9 = \{\bigcup_{bo=1}^{n_9} BC_{9,bo}\} = \boldsymbol{M} = \{\bigcup_{bo=1}^{me} M_{bo}\},$$

де $n_9 = me$ – кількість можливих ідентифікаторів міри ризику ($\boldsymbol{BC}_9 \subseteq \boldsymbol{BC}$, $bo = \overline{1, me}$) .

Елемент ***P*** – «Імовірність» (***BC***$_{10}$ = ***P***), який може відображатися статистичними даними. При виникненні труднощів з отриманням статистичних даних або для простоти інтерпретації величин, експерти часто використовують логіко-лінгвістичний підхід. З його допомогою здійснюється відображення відповідної характеристики за допомогою ЛЗ «ІМОВІРНІСТЬ». Вона визначається базовою терм-множиною, наприклад

$$\boldsymbol{BC}_{10} = \{\bigcup_{bo=1}^{n_{10}} BC_{10,bo}\} = \boldsymbol{P} = \{\bigcup_{bo=1}^{p} \underset{\sim}{P}_{bo}\},$$

де $n_{10} = p$ – кількість термів ЛЗ «ІМОВІРНІСТЬ», для членів якого справедливо відношення порядку $\underset{\sim}{P}_1 < \underset{\sim}{P}_2 < ... < \underset{\sim}{P}_p$ ($\boldsymbol{BC}_{10} \subseteq \boldsymbol{BC}$, $bo = \overline{1, p}$). Як правило, для зазначених НЧ на основі відомих методів формуються необхідні функції належності (ФН). Також, крім зазначених, можуть бути введені й інші значення первинних термів, наприклад, «дуже низька», «вище середнього», «нижче середнього» та ін. Очевидно, що в цьому випадку характеристика ***P*** відображається набором лінгвістичних значень, але як окремий випадок, вона може приймати чітке або інтервальне значення.

Елемент ***SC*** – «Ситуація вибору» ($\boldsymbol{BC}_{11}$ = ***SC***), який представляється ЛЗ «СИТУАЦІЯ ВИБОРУ» з базовою терм-множиною

$$\boldsymbol{BC}_{11} = \{\bigcup_{bo=1}^{n_{11}} BC_{11,bo}\} = \boldsymbol{SC} = \{\bigcup_{bo=1}^{sc} \underset{\sim}{SC}_{bo}\},$$

де $n_{11} = sc$ – кількість термів зазначеної ЛЗ, для яких справедливо відношення порядку $\underset{\sim}{SC}_1 < \underset{\sim}{SC}_2 < ... < \underset{\sim}{SC}_{sc}$ ($\boldsymbol{BC}_{11} \subseteq \boldsymbol{BC}$, $bo = \overline{1, sc}$).

Елемент ***V*** – «Вразливість» ($\boldsymbol{BC}_{12}$ = ***V***), який можна відобразити підмножиною ідентифікаторів вразливостей

$$\boldsymbol{BC}_{12} = \{\bigcup_{bo=1}^{n_{12}} BC_{12,bo}\} = \boldsymbol{V} = \{\bigcup_{bo=1}^{n} V_{bo}\},$$

де $n_{12} = n$ – кількість можливих вразливостей (і відповідно їх ідентифікаторів) РІС ($\boldsymbol{BC}_{12} \subseteq \boldsymbol{BC}, bo = \overline{1, n}$).

Елемент ***VA*** – «Оцінка CVSS» ($\boldsymbol{BC}_{13}$ = ***VA***), який може відображатися підмножиною,

$$\boldsymbol{BC}_{13} = \{\bigcup_{bo=1}^{n_{13}} BC_{13,bo}\} = \boldsymbol{VA} = \{\bigcup_{bo=1}^{va} VA_{bo}\},$$

де $n_{13} = va$ – кількість версій CVSS ($\boldsymbol{BC}_{13} \subseteq \boldsymbol{BC}$, $bo = \overline{1, va}$), наприклад, при *va* = 2

$$\boldsymbol{BC}_{13} = \{\bigcup_{bo=1}^{n_{13}} BC_{13,bo}\} = \{BC_{13,1}, BC_{13,2}\} =$$

$$= \boldsymbol{VA} = \{\bigcup_{bo=1}^{2} VA_{bo}\} = \{VA_1, VA_2\} = \{\text{«CVSS v02», «CVSS v03»}\},$$

($BC_{13,1} = VA_1$, $BC_{13,2} = VA_2$ – ідентифікатори версії CVSS). Цей елемент відображає наявність в системі версії CVSS оцінки.

На основі множини ***BC***, а також з урахуванням результатів аналізу проведеного в розділі 1, пропонується формувати дві базові підмножини:

– перша ідентифікуюча –

$$\{\bigcup_{i=1}^{ind} \boldsymbol{ABC}_i\} = \{\bigcup_{i=1}^{ind}\{\bigcup_{bo=1}^{abc_i} ABC_{i,bo}\}\} = \{\bigcup_{i=1}^{ind}\{ABC_{i,1}, ABC_{i,2}, ..., ABC_{i,abc_i}\}\} =$$

$$= \{\{ABC_{1,1}, ABC_{1,2}, ..., ABC_{1,abc_1}\},\ \{ABC_{2,1}, ABC_{2,2}, ..., ABC_{2,abc_2}\}, ...,$$

$$\{ABC_{ind,1}, ABC_{ind,2}, ..., ABC_{ind,abc_{ind}}\}\},\ (\boldsymbol{ABC}_i \subseteq \boldsymbol{BC},\ i = \overline{1,ind},\ bo = \overline{1,abc_i});$$

– друга оціночна –

$$\{\bigcup_{i=1}^{ass} \boldsymbol{SBC}_i\} = \{\bigcup_{i=1}^{ass}\{\bigcup_{bo=1}^{sbc_i} SBC_{i,bo}\}\} = \{\bigcup_{i=1}^{ass}\{SBC_{i,1}, SBC_{i,2}, ..., SBC_{i,sbc_i}\}\} =$$

$$= \{\{SBC_{1,1}, SBC_{1,2}, ..., SBC_{1,sbc_1}\},\ \{SBC_{2,1}, SBC_{2,2}, ..., SBC_{2,sbc_2}\}, ...,$$

$$\{SBC_{ass,1}, SBC_{ass,2}, ..., SBC_{ass,sbc_{ass}}\}\},\ (\boldsymbol{SBC}_i \subseteq \boldsymbol{BC},\ i = \overline{1,ass},\ bo = \overline{1,sbc_i}),$$

де *ind* та *ass* – відповідно кількість ідентифікуючих і оціночних характеристик ризику ІБ, які використовуються для його аналізу і оцінювання. Далі, для ефективної організації процесу аналізу існуючих засобів оцінювання та їх розробки здійснюється інтеграція членів представлених підмножин характеристик ризику за допомогою їх відображення в двох фіксованих кортежах (рис. 1). Перший кортеж – аналітичний (АК), який використовується для аналізу засобів оцінювання з метою подальшого їх вибору. Другий кортеж – синтетичний (СК), що використовується для допомоги розробникам, які синтезують такі засоби оцінювання.

Також розроблено методи інкрементування (збільшення) та декрементування (зменшення) порядку ЛЗ. Як було визначено засоби аналізу і оцінювання ризиків ІБ, які грунтуються на нечіткій логіці, використовують ЛЗ з фіксованою кількістю терм-множин, визначених експертами на етапі ініціалізації базових величин при налаштуванні системи. Для підвищення ефективності функціонування таких систем були представлені методи зменшення і збільшення числа термів ЛЗ для трапецієподібних і трикутних НЧ, на один порядок та їх модифікацій n-кратним розширенням, які дозволяють зменшувати чи збільшувати порядок ЛЗ без залучення експертів відповідної предметної області. Методи інкрементування реалізуються у чотири етапи: пошук коригувальних параметрів, визначення номера вершини, яка буде розширюватися, обчислення значень абсцис та нормування еталонів. Методи декрементування реалізовуються в три етапи: формування бази, розширення бази та часткове розширення бази. Для інкрементування ЛЗ на один порядок введена аналітична функція FT^{+1}, а для декрементування FT^{-1}. Також функція декрементування ЛЗ на один порядок модифікована *n*-кратною функцією FT^{-n}. Всі ці функції застосовуються для трансформування параметричних НЧ, а саме трапецієподібних та трикутних.

У третьому розділі з метою спрощення розрахунків ризиків і удосконалення методів розглядається інтегрований метод ОР, який на відміну від відомих, надає можливість оперувати одночасно чіткими і нечіткими параметрами з вибором необхідної кількості терм-множин. При цьому їх зміна не впливає на кінцевий результат і при тих же вхідних параметрах він залишається адекватним. Запропонований метод реалізується за десять кроків. Ступінь ризику в методі визначається за формулою:

$$dr^{(A_a)} = \sum_{j=1}^{m}\left(dr_j \sum_{i=1}^{q} LS_i \lambda_{ij}^{(A_a)} \right), \quad (4)$$

де dr_j=90-20(j-1), ($j = \overline{1,m}$) LS_i – рівень значущості оціночного компонента ($i = \overline{1,g}$), а величина $\lambda_{ij}^{(A_a)}$ визначається для кожної загрози A_a ($a = \overline{1,n}$) за формулами:

$$\lambda_{i1}^{(A_a)} = \begin{cases} 1 \text{ при } ek_i^{A_a} \in [bi_{11}, bi_{12}[\\ 0 \text{ при } ek_i^{A_a} \notin [bi_{11}, ci_1[\\ \mu_1(ek_i^{A_a}) \text{ при } ek_i^{A_a} \in [bi_{12}, ci_1[\end{cases}, \quad \lambda_{ij}^{(A_a)} = \begin{cases} \mu_j(ek_i^{A_a}) \text{ при } ek_i^{A_a} \in [ai_j, bi_{1j}[\\ 1 \text{ при } ek_i^{A_a} \in [bi_{1j}, bi_{2j}[\\ \mu_j(ek_i^{A_a}) \text{ при } ek_i^{A_a} \in [bi_{2j}, ci_j[\\ 0 \text{ при } ek_i^{A_a} \notin [ai_j, ci_j[\end{cases},$$

$$\lambda_{im}^{(A_a)} = \begin{cases} \mu_m(ek_i^{A_a}) \text{ при } ek_i^{A_a} \in [ai_m, bi_{1m}[\\ 1 \text{ при } ek_i^{A_a} \in [bi_{1m}, bi_{2m}[\\ 0 \text{ при } ek_i^{A_a} \notin [ai_m, bi_{2m}[\end{cases}, \quad j = \overline{2, m-1}, \quad (5)$$

де $ek_i^{A_a}$ – поточне значення оціночного компонента, а $\mu(dr)$ – функція належності нечіткій множині.

Після оцінки $dr^{(A_a)}$ проводиться лінгвістичне розпізнавання отриманих значень за допомогою ЛЗ «СТУПІНЬ РИЗИКУ», яка визначається кортежем <***DR***, $\underset{\sim}{T}_{DR}$, $\underset{\sim}{X}_{DR}$>, де базові терм-множини задаються m термами $\underset{\sim}{T}_{DR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{DR_j}$ за виразом:

$$SP^{(A_a)} = \begin{cases} (dr^{(A_a)}; \underset{\sim}{T}_{DR_j}) \text{ при } \mu_j(dr) = 1 \\ (dr^{(A_a)}; \underset{\sim}{T}_{DR_j}(\mu_j(dr)); \underset{\sim}{T}_{DR_{j+1}}(\mu_{j+1}(dr))) \text{ при } \mu_j(dr), \mu_{j+1}(dr) \neq 1 \end{cases}, \quad (6)$$

де $(dr^{(A_a)}; \underset{\sim}{T}_{DR_j})$ словесно інтерпретується, як – ступінь ризику $\underset{\sim}{T}_{DR_j}$ з числовим еквівалентом $dr^{(A_a)}$, а $(dr^{(A_a)}; \underset{\sim}{T}_{DR_j}(\mu_j(dr)); \underset{\sim}{T}_{DR_{j+1}}(\mu_{j+1}(dr)))$, як – ступінь ризику з числовим еквівалентом $dr^{(A_a)}$ межує між $\underset{\sim}{T}_{DR_j}$ та $\underset{\sim}{T}_{DR_{j+1}}$ з впевненістю експерта з межею $\underset{\sim}{T}_{DR_j} - \mu_j(dr)$ і $\underset{\sim}{T}_{DR_{j+1}} - \mu_{j+1}(dr)$.

Також за виразом

$$dr^{(cp)} = (\sum_{a=1}^{m} dr^{(A_a)}) / m \quad (7)$$

можна визначити середнє значення $dr^{(cp)}$ за оцінюваним РІС.

Також було удосконалено модель процесу синтезу систем оцінювання ризиків. Розроблено структурно-функціональну модель інтегрованої адаптованої системи ОР безпеки РІС. Модель процесу синтезу адаптивних систем ОР безпеки РІС (рис. 2) заснована на логіко-лінгвістичному підході, розроблених методах і БІМ та формується дванадцятьма етапами:

1) вибір методу ОР;

2) визначення базових параметрів для розробки систем ОР та оціночних компонентів за допомогою СК, який складається з 8-ми елементів $\boldsymbol{EP_i} \in \{\boldsymbol{EP}_i\}=\{\boldsymbol{AES, CA, D, E, F, L, P, V}\}$ $(i=\overline{1,g})$ (де i – показник (номер) поточного ідентифікатора оціночного компонента, а g – кількість таких компонентів);

3), 4) і 5) ідентифікація РІС IP_h (де $h=\overline{1,r}$, h – показник (номер) поточного ідентифікатора РІС, а r – кількість РІС), загроз або вразливостей $\mathrm{A} \in \{A_a\}$ $(a=\overline{1,n})$ / $\boldsymbol{V} = \{\bigcup_{bo=1}^{n} V_{bo}\}$, (де $bo=\overline{1,n}$, a / bo – показник (номер) поточного ідентифікатора загрози/вразливості, а n – кількість загроз/кількість можливих вразливостей (і відповідно їх ідентифікаторів) РІС), порушень базових характеристик ІБ $\mathrm{E} \in \{E_e\}$ (де $e=\overline{1,7}$, e – показник (номер) поточного ідентифікатора порушення базових характеристик ІБ);

6) формування множини параметрів, а саме ступеня ризику (СР) – ЛЗ «СТУПІНЬ РИЗИКУ» (***DR***), яка відповідає кортежу <***DR***, $\underset{\sim}{T}_{DR}$, $\underset{\sim}{X}_{DR}$>, для якого задається її базова терм-множина $\underset{\sim}{T}_{DR}=\bigcup_{j=1}^{m}\underset{\sim}{T}_{DR_j}$ $(j=\overline{1,m})$, (де m – кількість термів) та рівень оціночних компонентів (РОК) – ЛЗ «РІВЕНЬ ОЦІНОЧНОГО КОМПОНЕНТА $\boldsymbol{EP}_i$», яка визначається кортежем < $\boldsymbol{K}_{EP_i}$, $\underset{\sim}{T}_{K_{EP_i}}$, $\underset{\sim}{X}_{EP_i}$ >, де базові терм-множини задаються m термами $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}}=\bigcup_{j=1}^{m}\underset{\sim}{T}_{K_{EP_i j}}$;

7) вибір методу трансформування термів зазначених ЛЗ;

8) визначення рівня значущості LS_i ($i=\overline{1,g}$) за виразом

$$\boldsymbol{LS}_i = \frac{2(g-i+1)}{(g-1)g} \text{ або } \boldsymbol{LS}_i = 1/g \text{ ;}$$

9) по кожному визначеному на етапі 2 оціночному параметру $\{\boldsymbol{EP}_i\}$ ($i=\overline{1,g}$), з використанням сформованих на 6 етапі інтервалів і термів $\boldsymbol{K}_{EP_i}$, експерти відповідної предметної області визначають ***ek*** для усіх A_a/V_{bo} ($a=\overline{1,n}$, $bo=\overline{1,n}$), ідентифікованих на 4 етапі, тобто { $\boldsymbol{ep}_i^{A_a/V_{bo}}$ };

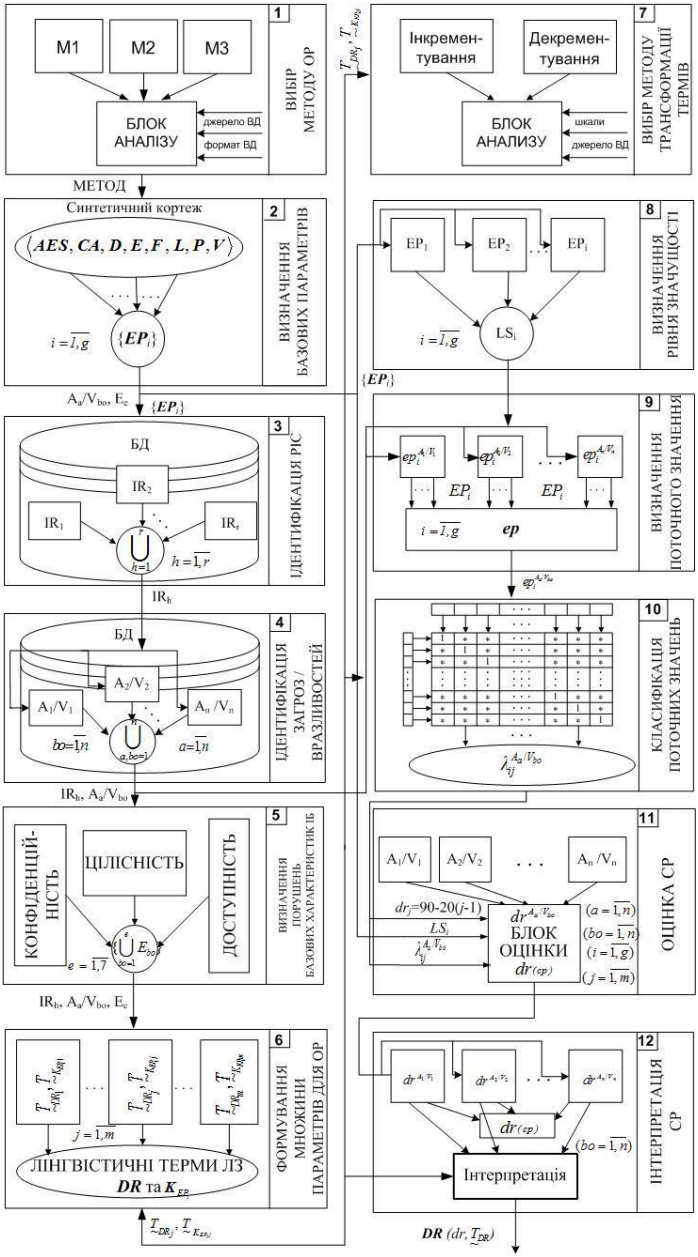

Рисунок 2 – Модель процесу синтезу адаптивних систем оцінки ризику безпеки РІС

10) класифікація поточних значень, а саме формується значення λ (див. опис методу);

11) та 12) оцінка $dr^{(A_u/V_{bo})}$, $dr^{(cp)}$ та інтерпретація СР.

Структурно-функціональна модель інтегрованої адаптивної системи оцінювання ризиків (рис. 3) містить підсистеми формування вхідних даних (ПСФВД) і обробки даних (ПСОД), модулі формування структурованого параметру, генерації звіту і служить для оперування одночасно чіткими і нечіткими параметрами з вибором необхідної кількості терм-множин, а зміна терм-множин не впливає на кінцевий результат і при тих же вхідних параметрах він залишається адекватним.

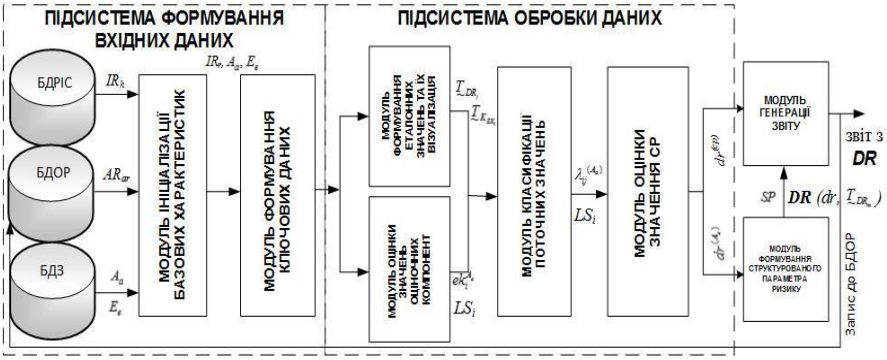

Рисунок 3 – Структурно-функціональна модель інтегрованої адаптивної системи ОР

У свою чергу ПСФВД служить для підготовки даних, заснованих на судженнях експертів для ПСОД і складається з: бази даних (БД) ресурсів інформаційних систем (БДРІС), БД загроз (БДЗ) і БД результатів ОР (БДОР); модуля ініціалізації базових характеристик; модуля формування ключових даних. Підсистема ПСОД містить модулі оцінки значень оціночних компонентів, формування еталонних значень та їх візуалізація, класифікації поточних значень оціночних компонентів і оцінки значення СР.

Четвертий розділ присвячений експериментальним дослідженням ПЗ ОР безпеки РІС та методів інкрементування та декрементування термів ЛЗ. На рис. 4 для прикладу наведені основні формули методів декрементування ЛЗ «СТУПІНЬ РИЗИКУ» (***DR***). Результати, отримані за допомогою методів інкрементування та декрементування термів лінгвістичної змінної, для різних типів розподілів параметричних трапецієподібних та трикутних нечітких чисел свідчить про коректність запропонованих методів.

На базі запропонованої БІМ та структурно-функціональної моделі відповідної системи розроблено алгоритм, інтегровані БД і на їх основі – прикладну програмну систему ОР безпеки РІС, яка відносно зведених даних дозволяє здійснювати ОР на основі прямого використання будь-яких (із зазначеної множини СК) параметрів.

З метою верифікації розроблених методів, моделі, структурного рішення і ПЗ, виконано перевірку, яка проводилася на основі моделювання декількох станів середовища оцінювання: 1-й стан – початкові умови зі встановленою кількістю загроз для РІС; 2-й стан – змінено кількість загроз для РІС; 3-й стан – блоковано одну

загрозу для РІС; 4-й стан – зміна значень оціночних компонентів (зменшення або збільшення).

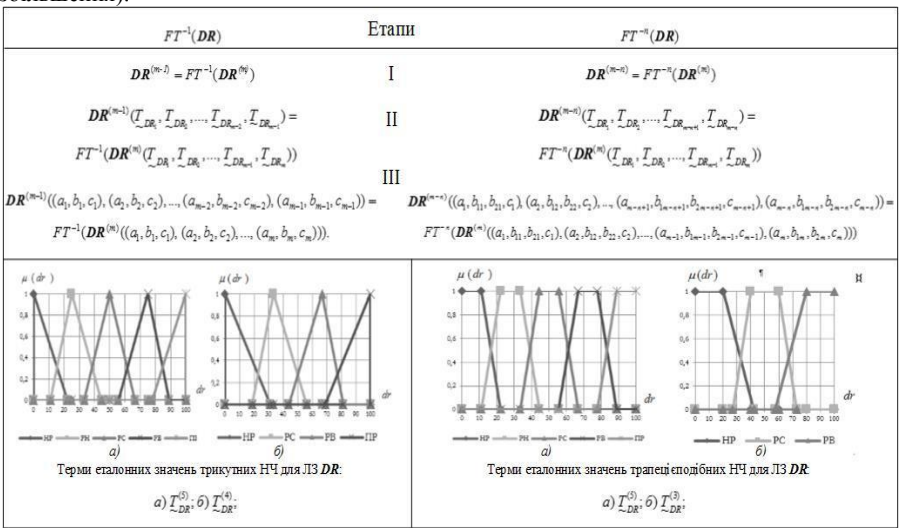

Рисунок 4 – Приклад використання методів декрементування ЛЗ

За допомогою розробленого ПЗ проведено моделювання роботи адаптивної системи ОР безпеки РІС. Для верифікації ПЗ виконано обчислення при середовищі оточення РІС з середнім, зниженим та підвищеним значенням ступеню ризику (табл. 2).

Таблиця 2

Порівняння середніх значень ступеню ризику $dr^{(cp)}$

PIC	$dr^{(cp)}$		
	Середній рівень ризику (початкові умови)	Знижений рівень ризику	Підвищений рівень ризику
IR₁	38,27 (РН (0,18), РС (0,82))	22 (РН)	53,4 (РС (0,66), РВ (0,34))
IR₂	12 (НР (0,8), РН (0,2))	10 (НР)	30,8 (РН (0,92), РС (0,08))
IR₃	43 (РС)	33,87 (РН (0,6), РС (0,4))	54,37 (РС (0,56), РВ (0,44))
IR₄	31,75 (РН (0,8), РС (0,2))	25,18 (РН)	42,21 (РС)

В результаті моделювання встановлено, що розроблені ПЗ адекватно реагують на зміну агресивності середовища оточення, а саме при його посиленні або ослаблені відповідно збільшується або зменшується значення ступеню ризику, а зміна терм-множин не впливає на кінцевий результат і при тих же вхідних параметрах він залишається адекватним.

У **додатках** знаходяться акти впровадження результатів дисертаційної роботи. Результати дисертації впроваджено у діяльність ТОВ «БІС «Дельта», а також використовуються у навчальному процесі кафедри безпеки інформаційних технологій Національного авіаційного університету та кафедри інформаційної безпеки Інституту

інформаційних та телекомунікаційних технологій Казахського національного дослідницького технічного університету ім. К.І. Сатпаєва.

ВИСНОВКИ

У дисертаційній роботі представлено результати дослідження, метою яких було створення адаптивної інтегрованої системи оцінювання ризиків безпеки ресурсів інформаційних систем у відповідності до запропонованої моделі процесу синтезу, яка заснована на створених методах і бістабільній інтегрованій кортежній моделі характеристик ризику, може бути представлена двома кортежами – аналітичним та синтетичним. У ході вирішення поставлених задач були отримані такі результати:

1. На основі удосконалення кортежної моделі створено бістабільну інтегровану кортежну модель характеристик ризику, яка за рахунок бістабільних відображень в аналітичному та статистичному кортежах з урахуванням необхідної множини початкових компонентів, дозволяє реалізовувати вибір відповідних інструментальних засобів і розробляти гнучкі та ефективні методи і системи оцінювання ризиків інформаційної безпеки.

2. Запропоновано базові методи інкрементування та декрементування порядку лінгвістичної змінної для систем оцінювання ризиків, які за рахунок використання аналітичних функцій зниження та збільшення термів, дозволяють реалізовувати трансформування базових еталонів параметрів без залучення експертів відповідної предметної галузі, що забезпечує адаптивність систем оцінювання ризиків.

3. Представлено інтегрований метод оцінювання ризиків безпеки ресурсів інформаційних систем, який на основі використання бістабільної інтегрованої кортежної моделі характеристик ризику, інтеграції детермінованого і нечіткого підходу та методів трансформування порядку лінгвістичної змінної, дозволяє створювати адаптивні засоби оцінювання ризиків, які використовують за вхідні дані динамічно змінювані набори детермінованих і нечітко визначених оціночних параметрів з урахуванням періоду часу, галузі, економічної та управлінської специфіки об’єкту захисту.

4. Удосконалено модель процесу синтезу систем оцінювання ризиків, яка за рахунок застосування розробленої бістабільної інтегрованої кортежної моделі характеристик ризику і представлених методів, дозволила формалізувати процес побудови адаптивних інструментальних засобів з гнучкими можливостями використання заданих множин величин при оцінюванні ризиків безпеки ресурсів інформаційних систем.

5. Розроблено структурно-функціональну модель інтегрованої адаптивної системи оцінювання ризиків, яка за рахунок підсистем формування вхідних даних і обробки даних, що реалізують запропоновані методи (інтегрований, інкрементування та декрементування), дозволяє перетворювати і формувати дані, як в якісній, так і в кількісній інтерпретації.

6. На базі запропонованої моделі процесу синтезу та структурно-функціональної моделі, розроблена адаптивна інтегрована система оцінювання ризиків безпеки ресурсів інформаційних систем, в якій для ефективного вирішенні завдань як в детермінованому, так і в нечіткому, слабоформалізованому середовищі, досягнута висока інтеграція функціональних можливостей, адаптивність і зручність використання.

7. Проведено експериментальне дослідження програмного забезпечення системи оцінювання ризиків з метою верифікації розроблених методів і моделей. Впровадження зазначених розробок підтвердило достовірність теоретичних гіпотез і висновків дисертаційної роботи.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Корченко А.Г. Метод преобразования эталонов параметров для систем анализа и оценивания рисков информационной безопасности / А.Г. Корченко, С.В. Казмирчук, А.Ю. Гололобов // Захист інформації. – 2013. – Т.15. – №4. – С. 359-366.
2. Казмирчук С.В. Интегрированный метод анализа и оценивания рисков информационной безопасности / С.В. Казмирчук, А.Ю. Гололобов // Захист інформації. – 2014. – Т.16. – №3. – С. 252-261.
3. Ахметов Б.С. Метод n-кратного понижения порядка лингвистических переменных на основе частного расширения базы / Б.С. Ахметов, С.В. Казмирчук, С.А. Гнатюк, Н.А. Сейлова, А.Ю. Гололобов, // Безпека інформації. – 2014. – Т.20. – №3. – С. 306-311.
4. Корченко А.Г. Метод n-кратного понижения числа термов лингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, Н.А. Сейлова, А.Ю. Гололобов // Защита информации. – 2014. – Т.16. – №4. – С. 284-291.
5. Корченко А.Г. Метод реализации функции трансформирования эталонов в задачах анализа и оценивания рисков / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, А.Ю. Гололобов // Безпека інформації. – 2015. – Т.21. – №1. – С. 306-311.
6. Корченко А.Г. Метод инкрементирования порядка лингвистических переменных для систем анализа и оценивания рисков / А.Г. Корченко, С.В. Казмирчук, Ю.Б. Коваленко, А.Ю. Гололобов // Захист інформації. – 2015. – Т.17. – №2. – С. 100-108.
7. Корченко А.Г. Бистабильная кортежная модель характеристик риска / А.Г. Корченко, С.В. Казмирчук, Ю.А. Дрейс, А.Ю. Гололобов // Захист інформації. – 2016. – №4. – С. 183-196.
8. Казмирчук С.В. Синтез систем оценивания рисков безопасности ресурсов информационных систем / С.В. Казмирчук, А.Ю. Гололобов, А. Арджомандифард // Вісник Інженерної академії України. – 2016. – №3. – С. 78-81.
9. Казмирчук С.В. Интегрированная адаптивная систем оценивания рисков безопасности ресурсов информационных систем / С.В. Казмирчук, А.Ю. Гололобов, М.С. Мовчан, Л.П. Рыбалко // Безпека інформації. – 2016. – Т.22. – №3. – С. 217-223.
10. Казмірчук С.В. Програмна система підтримки побудови моделі загроз / С.В. Казмірчук, А.Ю. Гололобов, К.В. Нікітіна // АВІА-2013: XI Міжнар. наук.-техн. конф., 21-23 трав. 2013 р.: Тези доп. – К., 2013. – С. 2.9–2.12.
11. Казмирчук С.В. Преобразования эталонов параметров для анализа и оценивания рисков / С.В. Казмирчук, А.Ю. Гололобов // Проблемы информатизации: I междунар. науч.-техн. конф., 19-20 декаб. 2013 г.: Тезисы докл. – Черкассы, 2013. – С. 24.
12. Казмирчук С.В. Метод трансформирования термов лингвистических переменных в задачах анализа и оценивания рисков информационной безопасности / С.В. Казмирчук, А.Ю. Гололобов // Радиоэлектроника и молодежь в XXI веке:

18-й Международный молодежный форум, 14-16 апр. 2014 г.: Тезисы докл. – Харьков, 2014. – Т. 9. – С. 77-78.

13. Корченко О.Г. Система оцінювання ризиків інформаційної безпеки / О.Г. Корченко, С.В. Казмірчук, А.Ю. Гололобов // Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2014): 6-та Всеукраїнська наук.-практ. конф., 09-12 верес. 2014 р.: Тези доп. – м. Миколаїв, 2014. – С. 44-48.

14. Корченко А.Г. Метод инкрементирования эталонов параметров для систем анализа и оценивания рисков / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, А.Ю. Гололобов // Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2015): 7-ма Всеук. наук.-практ. конф., 09-12 черв. 2015 р.: Тези доп. – м. Миколаїв, 2015. – С. 65-68.

15. Корченко А.Г. Представление эталонов параметров лингвистических переменных для систем анализа и оценивания рисков информационной безопасности / А.Г. Корченко, С.В. Казмирчук, А.Ю. Гололобов // Актуальні питання забезпечення кібернетичної безпеки та захист інформації: наук.-практ. конф., 25-28 лют. 2015 р.: Тези доп. – К., 2015. – С. 70-75.

АНОТАЦІЯ

Гололобов А.Ю. Методи і моделі адаптивних систем оцінки ризиків. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Національний авіаційний університет, Київ, 2017.

Дисертаційна робота присвячена вирішенню актуальної наукової задачі розробки методів і засобів оцінки ризику (ОР) безпеки ресурсів інформаційних систем (РІС), які дозволяють на основі використання бістабільної інтегрованої кортежної моделі (БІМ) характеристик ризику та методів трансформування порядку лінгвістичної змінної, створювати гнучкі, адаптивні засоби оцінювання.

Розроблено модель БІМ, що дозволяє динамічно визначати набори величин і таким чином забезпечити гнучкість розроблюваних засобів ОР безпеки РІС. Представлено методи інкрементування і декрементування порядку лінгвістичних змінних, які дозволяють проводити трансформування еталонів параметрів без залучення експертів відповідної предметної області. Розроблено інтегрований адаптивний метод ОР, який за рахунок моделі БІМ та трансформування еталонів параметрів, дозволяє створювати ефективні, адаптивні засоби оцінювання та використовувати в якості вхідних даних динамічно змінювані набори детермінованих і нечітко визначених оціночних параметрів. На підставі запропонованих методів і моделі БІМ, розроблено модель процесу синтезу адаптивних систем ОР безпеки РІС, яка дозволяє формалізувати і узагальнити процес побудови як програмних, так і програмно-апаратних систем, призначених для ефективного ОР. Розроблена нова структурно-функціональна модель системи, яка використовує запропоновані методи, моделі БІМ та процесу синтезу для вирішення завдань в галузі оцінки інформаційних ризиків.

Ключові слова: оцінка ризику, ресурси інформаційних систем, інкрементування, декрементування, інтегрований адаптивний метод, характеристики ризику.

АННОТАЦИЯ

Гололобов А.Ю. Методы и модели адаптивных систем оценки рисков. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – «Системы защиты информации». – Национальный авиационный университет, Киев, 2017.

Диссертационная работа посвящена решению актуальной научной задачи разработке методов и средств оценивания рисков безопасности ресурсов информационных систем, позволяющих на основе использования бистабильной интегрированной кортежной модели характеристик риска и методов трансформации порядке лингвистической переменной, создавать гибкие, адаптивные средства оценивания.

В работе проанализировано и исследовано существующие методы и программные средства оценивания рисков, с целью определения набора идентифицирующих и оценочных компонентов, используемых для создания и выбора наиболее эффективного инструментария решения соответствующих задач защиты информации. На основе усовершенствования кортежной модели создано бистабильная интегрированная кортежная модель характеристик риска, которая за счет, бистабильных отражений в аналитическом и статистическом кортежах с учетом необходимого множества начальных компонентов, позволяет реализовывать выбор соответствующих существующих инструментальных средств и разрабатывать гибкие и эффективные методы и системы оценивания рисков информационной безопасности.

Предложены базовые методы инкрементирования и декрементирования порядка лингвистической переменной для систем оценивания рисков, которые за счет использования аналитических функций уменьшения и увеличения числа термов, позволяют реализовывать трансформирование базовых эталонов параметров без привлечения экспертов соответствующей предметной отрасли, что обеспечивает адаптивность систем оценивания рисков.

Разработан интегрированный адаптивный метод оценивания рисков, который за счет бистабильной интегрированной кортежной модели характеристик риска и трансформирования эталонов параметров позволяет создавать эффективные средства оценивания, использующие в качестве входных данных динамически изменяемые наборы детерминированных и нечетко определенных оценочных параметров. Метод позволяет также рассчитывать риски, как на основе статистических данных, так и на экспертных оценках, сделанных в неопределенной, слабоформализованной среде с учетом периода времени, отрасли, экономической и управленческой специфики предприятия и др.

На основании предложенных методов и бистабильной интегрированной кортежной модели характеристик риска, усовершенствована модель процесса синтеза систем оценивания рисков, которая позволила за счет применения разработанной бистабильной интегрированной кортежной модели характеристик риска и предложенных методов, сформировать процесс построения адаптивных

инструментальных средств с гибкими возможностями использования заданных множеств величин при оценивании рисков безопасности ресурсов информационных систем.

Разработана структурно-функциональная модель интегрированной адаптивной системы оценивания рисков, которая за счет подсистем формирования входных данных и обработки данных, которые реализуют предложенные методы (интегрированный, инкрементирования и декрементирования), позволяет преобразовывать и формировать данные, как в качественной, так и в количественной интерпретации.

На основе предложенной модели синтеза и структурного решения, разработана система оценивания рисков безопасности ресурсов информационных систем, в которой достигнута высокая интеграция функциональных возможностей, адаптивность, гибкость и удобство использования для эффективного решении заданий, как в детерминированной, так и в нечеткой слабоформализованной среде.

Ключевые слова: оценка риска, ресурсы информационных систем, инкрементирования, декрементирования, интегрированный адаптивный метод, характеристики риска.

ABSTRACT

Hololobov A.Yu. The methods and models of adaptive risks assessment systems. – Manuscript.

The dissertation is intended to proceed with PhD degree on the specialty 05.13.21 «Information security systems» National Aviation University. – Kyiv, 2017.

Dissertation work is sanctified to the decision of actual scientific task of development of assessment risks (AR) of information systems resources (ISR) methods and facilities basis of the use of the descriptions risk bistable integrated cortege model (BIM) and order transformation methods of linguistic variable (LV) to create flexible, adaptive facilities of evaluation.

The model of BIM, allowing dinamically to determine the sets of sizes and thus to promote flexibility and adaptivity of the corresponding developed facilities of AR of safety ISR is worked out. The incrementation and decrementation methods of linguistic variables order, that allow to conduct transforming of standards of parameters without using corresponding subject domain experts, are presented. The integrated adaptive method of AR, that due to the model of BIM and transforming of standards of parameters allows to create effective facilities evaluations using as datains the dynamically changeable sets of the estimated parameters both in determined, and in fuzzy is worked out. On the basis of the offered methods and BIM, the model of process of synthesis of the adaptive systems of AR of safety allowing formalize and generalize the process of construction both programmatic and programmatic hardware-based systems intended for effective AR is worked out. The new structural decision of the system, using the offered methods, models of BIM and process of synthesis for the decision of tasks in informative risks assessment area is presented.

Key words: risk assessment, informative systems resources, incrementation, decrementation, integrated adaptive method, characteristics of risk.