© Gizun A. The software complex for the detection and evaluation of crisis situations in the information field // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 2, p.137-146.

DOI: 10.18372/2225-5036.24.13038

ПРОГРАМНИЙ КОМПЛЕКС ВИЯВЛЕННЯ ТА ОЦІНЮВАННЯ КРИЗОВИХ СИТУАЦІЙ В ІНФОРМАЦІЙНІЙ СФЕРІ

Андрій Гізун

Національний авіаційний університет, Україна

ГІЗУН Андрій Іванович, к.т.н.

Рік та місце народження: 1987 рік, м. Нетішин, Хмельницька обл., Україна.
Освіта: Національний авіаційний університет, 2010 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки, комплексні системи захисту інформації, штучні імунні системи, управління безперервністю бізнесу та правове забезпечення захисту інформації.
Публікації: більше 80 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
E-mail: andriy.gizun@gmail.com

Анотація. *Забезпечення сталого розвитку людства та його безпекових аспектів на сьогодні тісно пов'язано з необхідністю управління інцидентами/потенційними кризовими ситуаціями. Зокрема, важливим є їх вчасне виявлення, ідентифікування та оцінювання. Так, виникнення різного роду інцидентів інформаційної безпеки можуть серйозно вплинути на бізнес-процеси будь-якого підприємства, а при досягненні рівня їх впливу на інформаційну систему певного критичного значення виникає можливість появи кризової ситуації. Особливий напрямок стратегічного менеджменту, який регулює процеси управління кризовими ситуаціями – їх виявлення, ідентифікацію, оцінювання, нейтралізацію, попередження та ліквідацію наслідків – управління безперервністю бізнесу бере свій початок ще в 80-их роках минулого сторіччя. Проте раніше в цій сфері переважали системи, основними функціями яких були лише підтримка інформаційних технологій в умовах кризи, нейтралізація чи ліквідація наслідків, документаційне забезпечення формування та виконання планів безперервності бізнесу. І лише зараз увагу почали акцентувати на процедурі раннього виявлення кризової ситуації чи оцінки її деструктивного впливу. Сучасні системи управління кризовими ситуаціями здебільшого використовують математичні моделі, засновані на теорії ймовірностей, ознакових та компараторних моделях, що мають ряд суттєвих недоліків. В цій роботі пропонується до уваги опис-програмного забезпечення, яке реалізує розроблений обчислювальний комплекс виявлення та оцінювання кризових ситуацій в інформаційній сфері, робота якого ґрунтується на використані нечітких слабоформалізованих моделей та методів з застосуванням експертних підходів. Такий комплекс дозволяє нівелювати основні недоліки відомих подібних рішень, в тому числі залежність від статистичних даних, швидкості їх обробки, неповноти та нечіткості вхідних даних. В даній статті описана програмна реалізації обчислювального комплексу виявлення та оцінювання кризових ситуацій в інформаційній сфері, його інтерфейс та функціонал, описані режими роботи та особливості застосування як в режимі реального часу, так і для моделювання кризових ситуацій різного роду.*

Ключові слова: *кризова ситуація, метод, система, вияивлення та оцінювання кризових ситуацій, концепція управління безперервністю бізнесу, нечітка логіка, програмне забезпечення, інтерфейс, функціонал, програмний модуль.*

Вступ

Зростаючі темпи інформатизації діяльності людства призводять до практично прямої і перманентної залежності всіх сфер людської цивілізації від безперервності інформаційних систем та технологій, яка може бути порушена широким діапазоном техногенних, соціальних, природних інцидентів, що за умов відсутності подальшого контролю можуть перерости в повноцінні кризові ситуації з колосальними економічними збитками, пораненнями та загибеллю людей, порушенням стану інформаційної захищеності підприємства, установи, регіону чи навіть цілої країни. Статистичні звіти останніх років підтверджують ріст кризових ситуацій, що впливають на людство, що відображено зокрема в [1].

Регулювання сфери моніторингу і управління кризовими ситуаціями (КС), що тим чи іншим чином впливають на роботу інформаційних систем здійснюється відносно новим напрямом стратегічного менеджменту, що отримав назву Управління безперервністю бізнесу, концептуальні основи були закладені в працях фахівців британських та американських організацій Business Continuity Institute (BCI) і Disaster Recovery Institute International (DRII). В пострадянських країнах цей менеджерський підхід

почав свій розвиток з публікації праці [2], де він був переосмислений і адаптований до реалій пострадянських держав. На сьогодні в технічному аспекті реалізована велика кількість технічних рішень, включаючи холодні та гарячі майданчики відновлення роботи IT-сервісів, системи резервного копіювання тощо. Загальний огляд та принцип їх роботи наведені в [3, 4].

Однак, досить мало досліджень, які б акцентували увагу не на реагуванні на кризові ситуації та усунені їх наслідків, а на проблемі раннього виявлення, ідентифікації та оцінці деструктивного впливу інцидентів потенційних кризових ситуацій (ІПКС). Не зважаючи на це, все ж деякі наукові напрацювання присутні в цій сфері. Зокрема спробу створити адекватні математичні моделі в цій сфері здійснив Качинський в [5] та ряд інших вітчизняних та закордонних науковців, які детально проаналізовано в роботі [6]. Проте варто зазначити, що майже всі вони мають ряд недоліків внаслідок залежності їх від процесу збору і обробки статистики та базування на основі компараторного принципу. В деякій мірі позбавляє цих недоліків застосування нечіткої логіки та експертних підходів, що запропоновано в [7]. Розвитком цих ідей стали праці, в яких запропоновані метод виявлення інцидентів/потенційних кризових ситуацій [8], метод оцінки рівня критичності для систем управління кризовими ситуаціями [9] та інтегрована модель представлення кризових ситуацій [10], в якій кризові ситуації описуються у вигляді кортежу, що складається з ідентифікатора кризової ситуації, його поточних ідентифікуючих та оціночних параметрів та їх еталонних значень, логіко-лінгвістичного правила для визначення ймовірності настання кризової ситуації та показника її критичності. на базі названих методів та моделі було запропоноване структурно-технічне рішення - Обчислювальний комплекс виявлення та оцінювання кризових ситуацій в інформаційній сфері [11], для автоматизації якого необхідна була його програмна реалізація

Тож метою даної статті є підвищення рівня автоматизації запропонованого комплексу виявлення та оцінювання кризових ситуацій в інформаційній сфері завдяки розробці відповідного програмного забезпечення (ПЗ), його опис і представлення інтерфейсу, можливостей та функціоналу щодо виконання безпосередніх функції комплексу в режимі реального часу або моделювання відповідних ситуації в рамках експериментальних досліджень.

Основна частина дослідження

Обґрунтування вибору середовища програмування

У якості середовища розробки програмних засобів обрано технологічну платформу 1С: Підприємство 8.3. Технологічна платформа надає об'єкти (даних і метаданих) і механізми управління об'єктами [12]. Слід впахувати, що з 2015 року в Україні заборонені окремі продукти 1С, але не саме середовище програмування. Об’єкти (дані та метадані) описуються у вигляді конфігурацій. При автоматизації будь-якої діяльності (розробці програмних засобів) складається своя конфігурація об'єктів, яка і являє собою закінчене прикладне рішення. Конфігурація створюється в спеціальному режимі роботи програмного продукту під назвою «Конфігуратор», потім запускається режим роботи під назвою «1С: Підприємство», в якому користувач отримує доступ до основних функцій, реалізованим в даному прикладному рішенні (конфігурації). Сама платформа не є програмним продуктом для використання кінцевими користувачами, а є фундаментом для розробки та роботи прикладних рішень.

Основні ключові можливості технологічної платформи 1С: Підприємства 8.3, які вплинули на вибір даного середовища [12}:

– можливість використання трьох клієнтських програм: Товстий клієнт, Тонкий клієнт, Веб-клієнт;

– багатоплатформеність. У версії 1С: Підприємство 8.3, завдяки появі веб-клієнта, всі компоненти системи можуть працювати на комп'ютерах як під управлінням Windows, так і під управлінням Linux;

– відмовостійкий масштабований кластер з динамічним розподілом навантаження. В 1С: Підприємстві 8.3 розвиток кластера серверів виконано відразу по декількох напрямках: масштабованість, відмовостійкість, динамічний розподіл навантаження;

– масштабованість. Можна управляти розподілом навантаження, яке раніше виконувалось єдиним менеджер кластеру. Відмовостійкість кластера в цілому досягається за рахунок того, що в 1С: Підприємство 8.3 кілька кластерів можуть бути об'єднані в групу резервування. Кластери, що знаходяться в одній групі резервування синхронізуються автоматично;

– відмовостійкість робочих процесів досягається за рахунок їх резервування. Динамічний розподіл навантаження;

– завантаженість робочих процесів аналізується динамічно і при необхідності клієнт автоматично перемикається на більш продуктивний робочий процес;

– новий інтерфейс. 1С: Підприємство 8.3 повністю змінює весь шар роботи з інтерфейсом, до якого відноситься командний інтерфейс, форми, віконна система;

– нова модель клієнт-серверної взаємодії. Архітектура керованого додатку орієнтована на максимальний перенос виконання всієї функціональності на сервер і максимальне «полегшення» клієнта. Функціональність форм і командного інтерфейсу також реалізована на сервері. На клієнті відображається вже підготовлена на сервері форма, виконується введення даних і виклики сервера для запису введених даних та інших необхідних дій. Аналогічно командний інтерфейс і звіти формується на сервері і відображається на клієнті.

Усі вище перечисленні можливості використання 1С: Підприємства 8.3 свідчать про те, що дана технологічна платформа може бути зручним засобом не тільки для автоматизації бухгалтерського та управлінського обліків підприємств, але й може знаходить своє застосування в областях, далеких від власне бухгалтерських завдань, наприклад для проведення наукових досліджень. Саме, тому дану пла-

тформу обрано для проведення експериментальних досліджень розроблених рішень.

Програмна система виявлення та ідентифікації потенційної критичної ситуації (СВІПКС)

Виконуваний програмний модуль може бути використаний на будь-якому комп'ютері, характеристики яких відповідають мінімальним вимогам для роботи із 1С Підприємством (1С Підприємство має бути встановлено на комп'ютері):

– процесор Intel Pentium IV/Xeon 2,4 ГГц і більше або AMD з аналогічними характеристиками;

– оперативна пам'ять 1024 Мб і більше;

– жорсткий диск 40 Гб і більше;

– ОС – Microsoft Windows.

Програмне забезпечення «СВІПКС v.1.0»

Структура розробленого програмного засобу (прикладного рішення) у режимі роботи «Конфігуратор» наведена на рис. 1.

Для проведення експериментального дослідження запропонованого комплексу в аспекті виявлення ІПКС на базі нечітких моделей було розроблено програмне забезпечення «*СВІПКС v.1.0*».

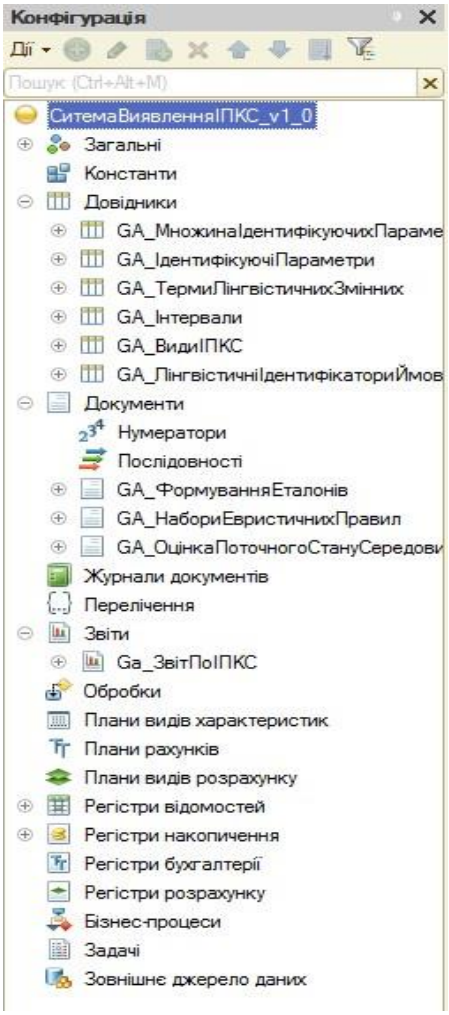

Рис. 1. Структура ПЗ «*СВІПКС v.1.0*» у режимі роботи «Конфігуратор»

Дане програмне забезпечення реалізує виявлення ІПКС різного характеру в умовах слабоформалізованого нечіткого середовища. В ньому реалізовані процеси побудови еталонів ідентифікуючих параметрів, наборів ЕП, фазифікації значень поточних параметрів та їх порівняння з еталонними за рахунок розрахунку узагальненої відстані Хемінга. В регістри системи заносяться ідентифікуючі параметри та ідентифікатори ІПКС, склад і кількість яких може коригуватися.

Інтерфейс програми представлений на рис. 2.

Як видно з рис. 1 − 2 розроблене ПЗ вміщує шість довідників і трьох документів. У середовищі 1С для роботи з постійною і умовно постійною інформацією з деякою множиною значень в системі використовуються об'єкти типу «Довідники». Для реалізації запропонованих математичних моделей були створені наступні об'єкти типу «Довідники»: «Множина ідентифікуючих параметрів», «Ідентифікуючі параметри», «Терми лінгвістичних змінних», «Інтервали», «Види ІПКС», «Лінгвістичні ідентифікатори можливості реалізації ІПКС». Через меню «Довідники» в інтерфейсі можна отримати доступ до цих довідників. Розглянемо названі довідники більш детально.

У довіднику «Множина ідентифікуючих параметрів» зберігаються множини (набори) ідентифікуючих параметрів, що використовується під час роботи системи для виявлення та ідентифікації ІПКС, та задається їх список. На рис. 3 наведено вікна форми елемента вказаного довідника.

Довідник «Ідентифікуючі параметри» використовується для зберігання всіх параметрів, що задіяні в роботі системи. Також у кожному параметрі вказуються його інтервали та терми лінгвістичних зміних (ЛЗ), що їх характеризують. На рис. 4 наведено вікна форми списку та форми елементу довідника «Ідентифікуючі параметри».

Довідники «Терми лінгвістичних змінних» та «Інтервали» використовується для зберігання інформації про вищевказані ЛЗ та інтервали. Довідник «Лінгвістичні ідентифікатори можливості реалізації ІПКС» призначений для зберігання інформації по всім лінгвістичним ідентифікаторам, що використовуються в дослідженні (приклад форми списку представлено на рис. 5).

Довідник «Види ІПКС» необхідний для зберігання переліку інцидентів, що виявлялися при експериментальному дослідженні, та відповідні їм ідентифікуючі параметри. На рис. 6 наведено вікно форми списку даного довідника.

В 1С за допомогою об'єктів типу «Документы» організовується введення в систему інформації про здійснення будь-яких операцій, а також їх перегляд і корегування. В розробленій конфігурації були створені наступні об'єкти типу «Документы»: «Формування еталонів», «Набори евристичних правил», «Оцінка поточного стану середовища». Через меню «Документы» в інтерфейсі можна отримати доступдо них. Еталони параметрів задаються експертом у документі «Формування еталонів» (приклад див. на рис. 7). На вкладці «Аналітичні дані параметра» заносяться експертні дані для формування еталонів за методом лінгвістичних термів на основі статистики (МЛТС). Програмний засіб автоматично будує графік функції належності еталонів лінгвістичної змінної.

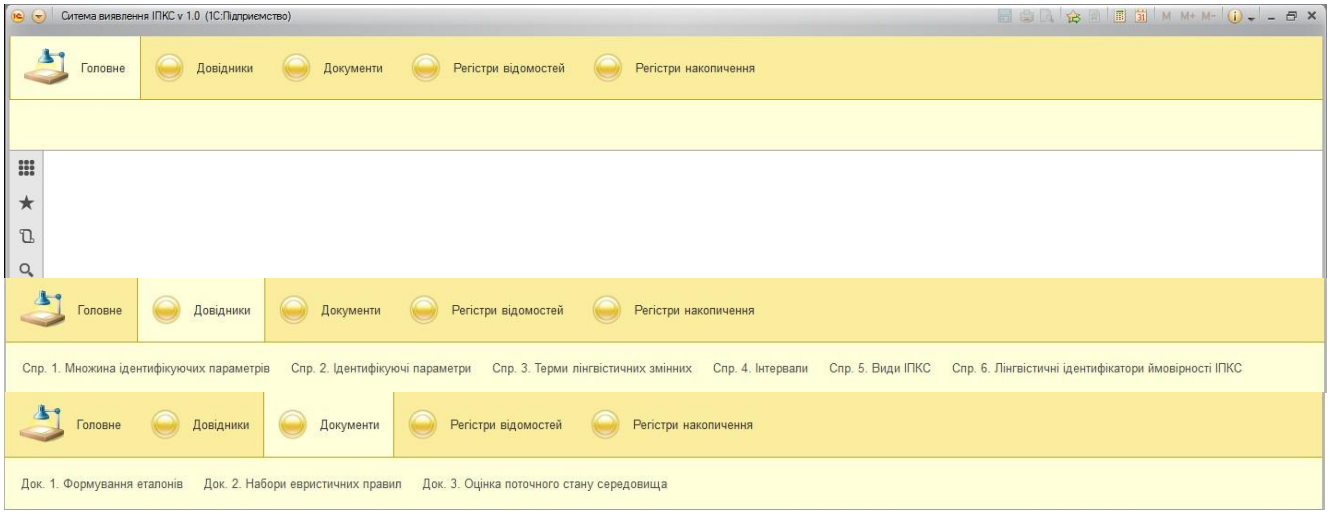

Рис. 2. Інтерфейс користувача ПЗ «*СВІПКС v.1.0*»

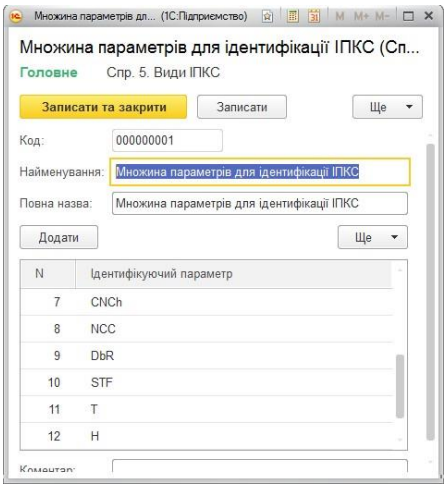

Рис. 3. Вікно форми елемента «Множина ідентифікуючих параметрів»

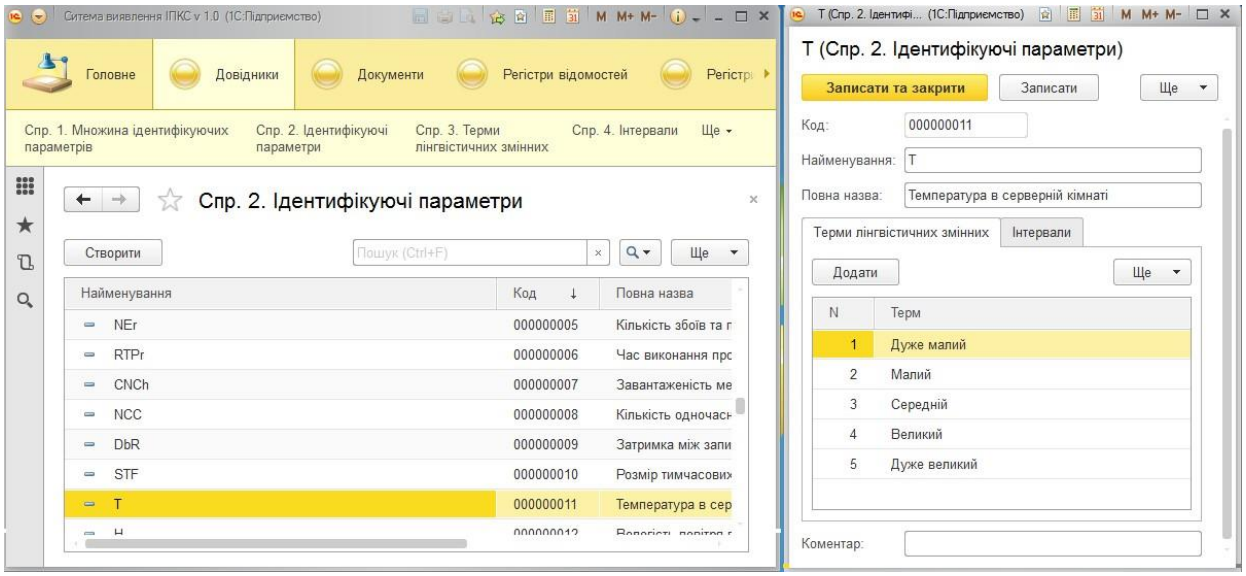

Рис. 4. Вікна форми списку та елемента довідника «Ідентифікуючі параметри»

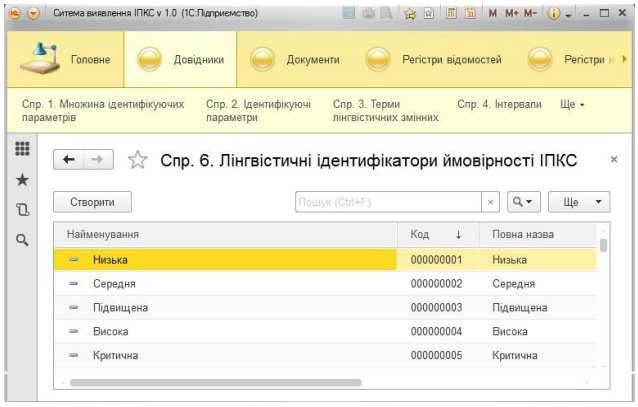

Рис. 5. Вікно форми списку довідника «Лінгвістичні ідентифікатори»

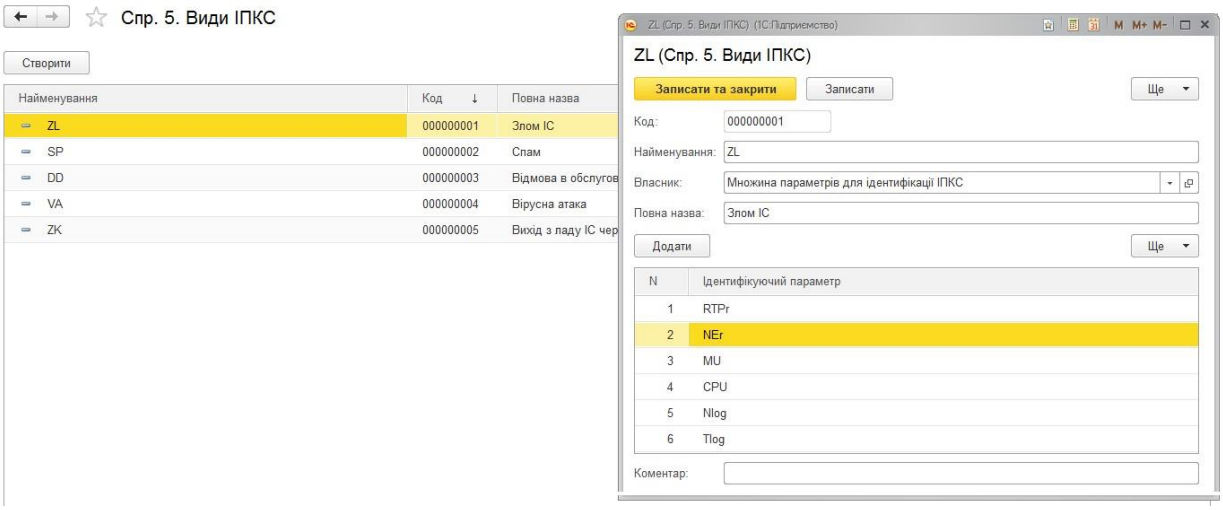

Рис. 6. Вікна форми списку та форми елемента довідника «Види ІПКС»

У документі «Набори евристичних правил» (рис. 8) на вкладці «Список параметрів» задаються параметри, що входять в відповідні правила щодо виявлення певного ІПКС, на вкладці «Лінгвістичні ідентифікатори» задаються лінгвістичні значення, які характеризують судження експерта щодо можливості реалізації ІПКС, на вкладці «Правила» формуються набори евристичних правил (ЕП) з зазначенням відповідного лінгвістичного ідентифікатора.

Документ «Оцінка поточного стану» безпосередньо реалізує експеримент. У формі елемента документа «Оцінка поточного стану» задається кількість серій експерименту в графі «Кількість записів стаститики», а також інші параметри (дата, множина параметрів, номер експерименту, кількість даних для групування під час фазифікації). На вкладці «Таблиця даних статистики» відображаються зібрані дані, а на вкладці «Таблиця згрупованих даних» відображені вже фазифіковані значеня і результуючий рівень можливості реалізації ІПКС з зазначенням його виду. Вікно форми елемента документа «Оцінка поточного стану» зображено на рис. 9.

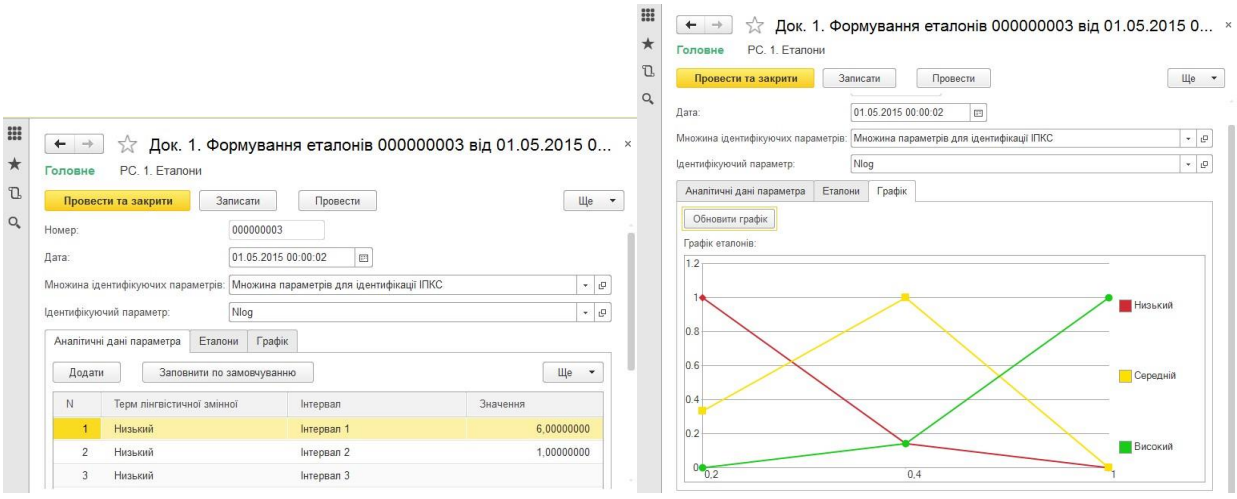

Рис. 7. Вікно форми елемента документа «Установка эталонов»

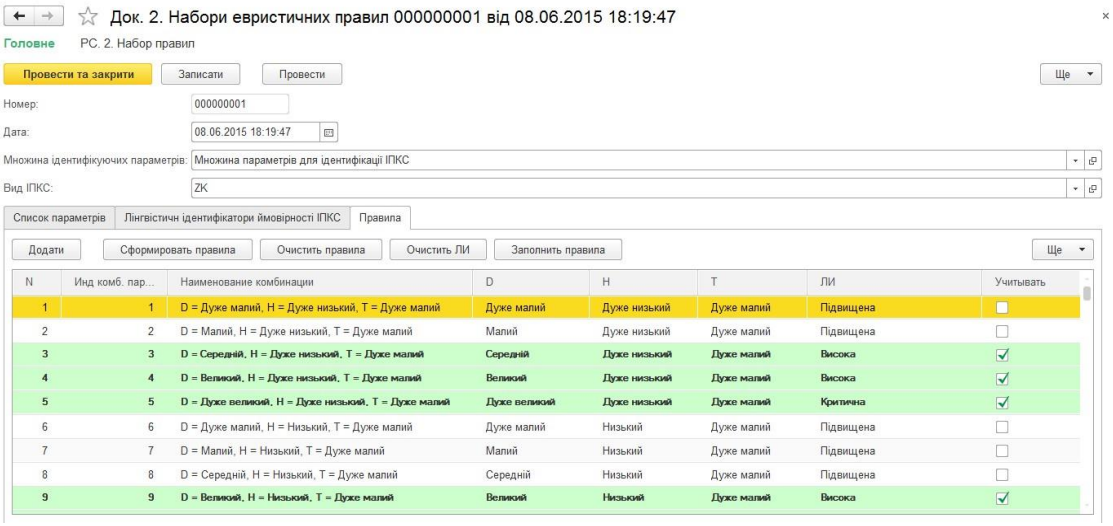

Рис. 8. Вікно форми елемента документа «Набори евристичних правил»

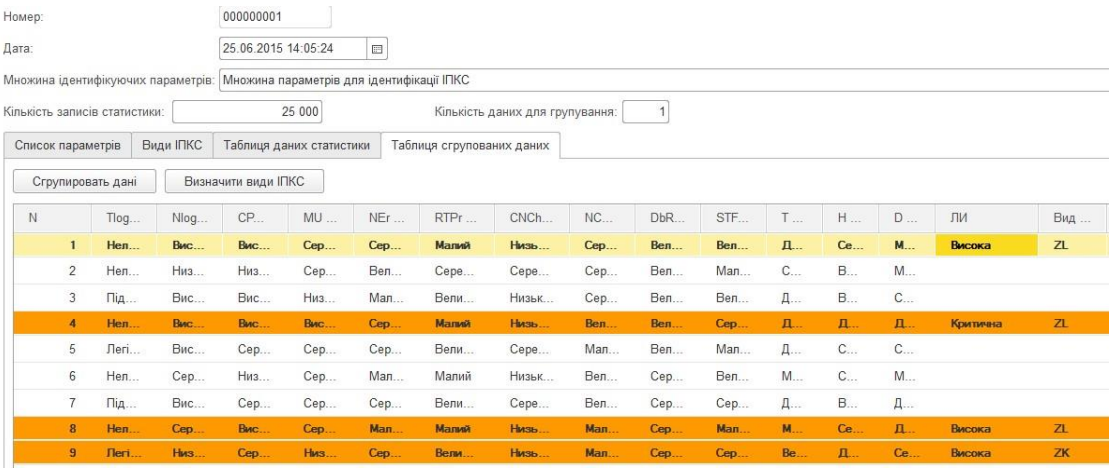

Рис. 9. Вікно форми елемента документа «Оцінка поточного стану»

У 1С звіти використовуються для отримання зведеної інформації на підставі даних, введених в системі. В розробленій конфігурації був створений один об'єкт типу «Звіти» − «Звіт по ІПКС». За допомогою даного звіту можна отримати доступ до детального звіту за результатами проведення імітаційного моделювання, що здійснюється програмним засобом.

Програмна система оцінки критичності ситуації (СОКС)

Виконуваний програмний модуль як і попередній може бути використаний на будь-якому комп'ютері, характеристики яких відповідають мінімальним вимогам для роботи із 1С Підприємством.

Програмне забезпечення «СОКС v.1.0»

Структура розробленого програмного засобу (прикладного рішення) у режимі роботи «Конфігуратор» наведена на рис. 10.

Для проведення експерименту, на основі методу оцінки критичності ситуації, було розроблено програмне забезпечення «*СОКС v.1.0*». Дане програмне забезпечення реалізує процес оцінювання рівня критичності ситуації, що сталася внаслідок впливу ІПКС різного характеру в умовах слабоформалізованого нечіткого середовища.

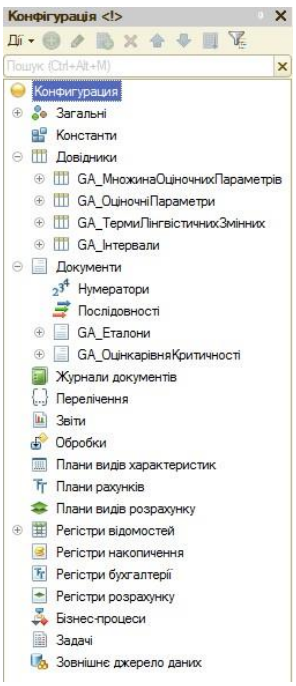

Рис. 10. Структура ПЗ «*СОКС v.1.0*» у режимі роботи «Конфігуратор»

В ньому реалізовані процеси побудови еталонів оціночних параметрів, визначення коефіцієнтів важливості і ранжування параметрів, фазифікації значень поточних параметрів, обрахунку показника рівня критичності, що представлений в формі нечіткого числа та їх дефазифікація для відображення в вигляді індикатора рівня критичності. В регістри системи заносяться оціночні параметри та експертні дані. Оціночні параметри в подальшому можуть бути скореговані.

Інтерфейс програми представлений на рис. 11. Як видно з рис. 10-11, розроблене ПЗ «*СОКС v.1.0*» вміщує чотири довідника і два документи. Для реалізації запропонованих математичних моделей були створені наступні об'єкти типу «Довідники»: «Множина оціночних параметрів», «Оціночні параметри», «Терми лінгвістичних змінних» та «Інтервали». Через меню «Довідники» в інтерфейсі можна отримати доступ до цих довідників. В розробленій конфігурації були створені наступні об'єкти типу «Документи»: «Еталони», «Оцінка рівня критичності». Через меню «Документы» в інтерфейсі можна отримати доступ до них.

У довіднику «Множина оціночних параметрів» визначаються параметри для оцінки рівня критичності, задається їх список та обраховуються коефіцієнти важливості в відповідних вкладках вікна форми елемента. На рис. 12 наведено вікна форми елемента вказаного довідника.

Довідник «Оціночні параметри» використовується для зберігання всіх параметрів, що задіяні в роботі системи. Також у кожному параметрі вказуються його інтервали та терми ЛЗ, що його характеризують. На рис. 13 наведено вікна форми списку та форми елементу довідника «Оціночні параметри».

Довідники «Терми лінгвістичних змінних» та «Інтервали» використовується для зберігання інформації про вищевказані ЛЗ та інтервали, на основі яких будуються еталони.

Еталони параметрів задаються експертом у документі «Еталони» (приклад див на рис. 14). На вкладці «Еталони» заносяться експертні дані для формування еталонів за параметричним методом. Програмний засіб автоматично будує графік функції належності еталонів лінгвістичної змінної, що відображується на вкладці «Графік».

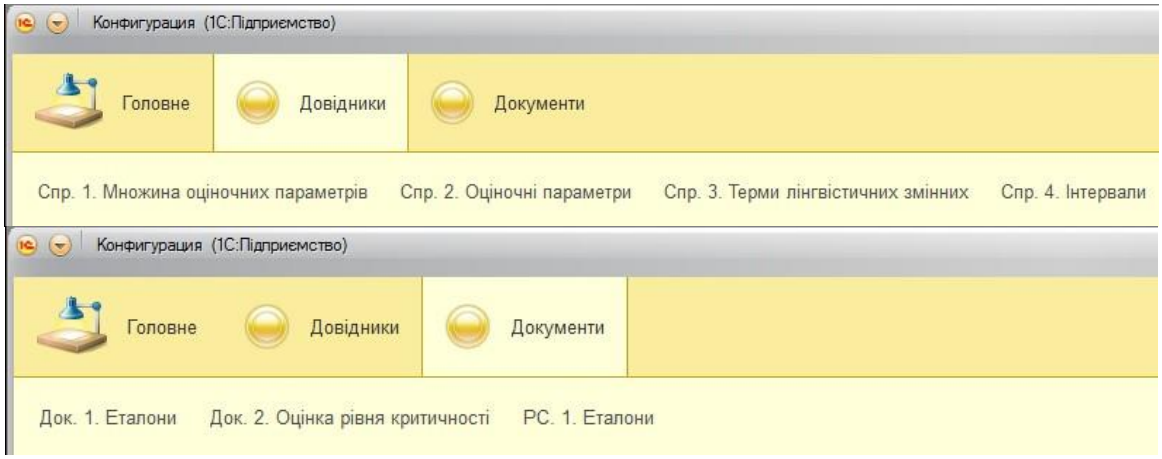

Рис. 11. Інтерфейс користувача ПЗ «*СОКС v.1.0*»

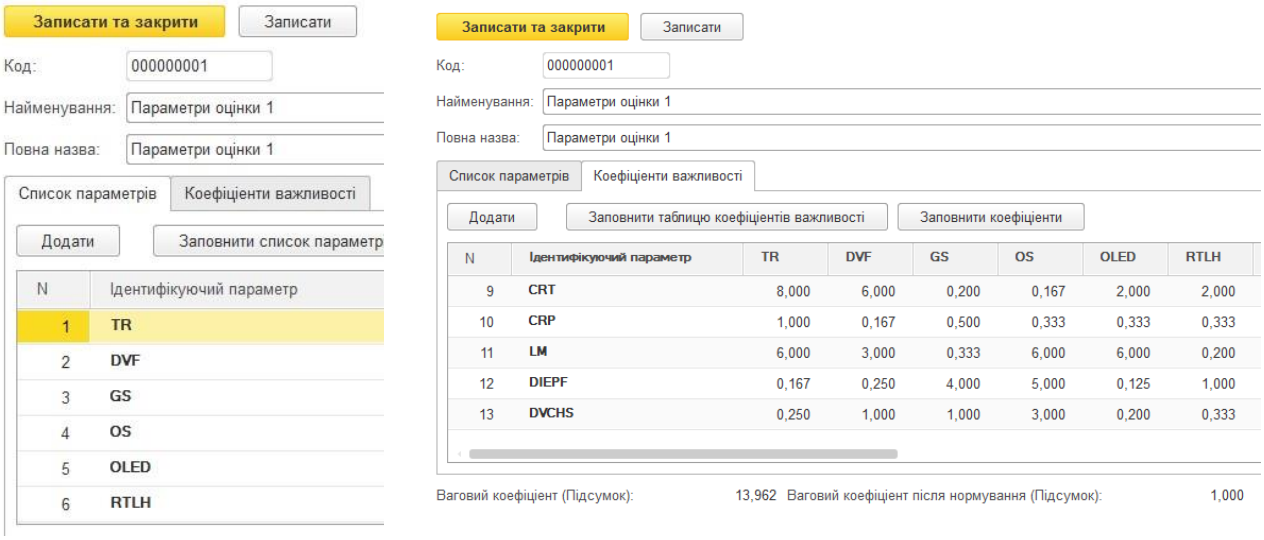

Рис. 12. Вікно форми елемента «Множина оціночних параметрів»

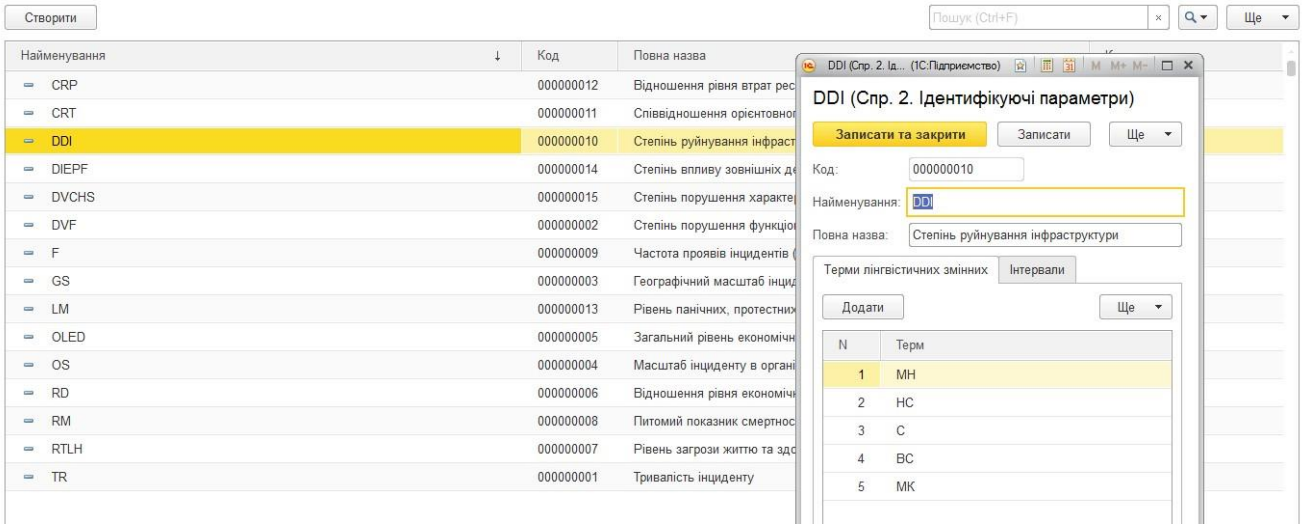

Рис. 13. Вікна форми списку та елемента довідника «Ідентифікуючі параметри»

Документ «Оцінка рівня критичності» безпосередньо реалізує експеримент і в ньому обчислюється поточний рівень критичності. У формі елемента документа «Оцінка рівня критичності» задається кількість вимірювань показника сенсорів в графі «Кількість даних для групування», а також інші параметри (дата, множина параметрів, номер експерименту). На вкладці «Список параметрів» вибираються параметри, по яким здійснюється оцінка рівня критичності. На вкладках «Таблиця даних статистики» і «Таблиця згрупованих даних» відображаються зібрані дані, та їх фазифіковані значення. Вкладка «Таблиця даних ЛЦС» відображає обрахований рівень критичності поточної ситуації в нечіткому вигляді, а вкладки «Таблиця розгрупованих даних» та «Таблиця розгрупованих даних ЛЦС» – значення оціночних параметрів та рівня критичності в чіткому вигляді після проведення процедури дефазифікації. На вкладці «Порівняння рівнів критичності» визначається відповідний поточному рівню критичності терм оціночного еталона через обрахунок УВХ. Вікно форми елемента документа «Оцінка поточного стану» зображено на рис. 15.

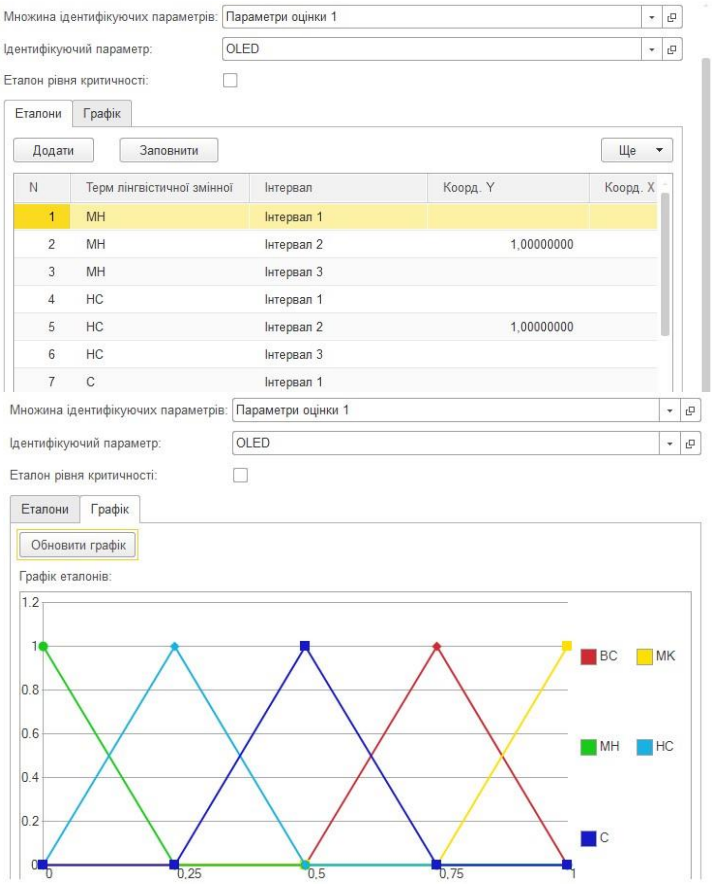

Рис. 14. Вікно форми елемента документа «Еталони»

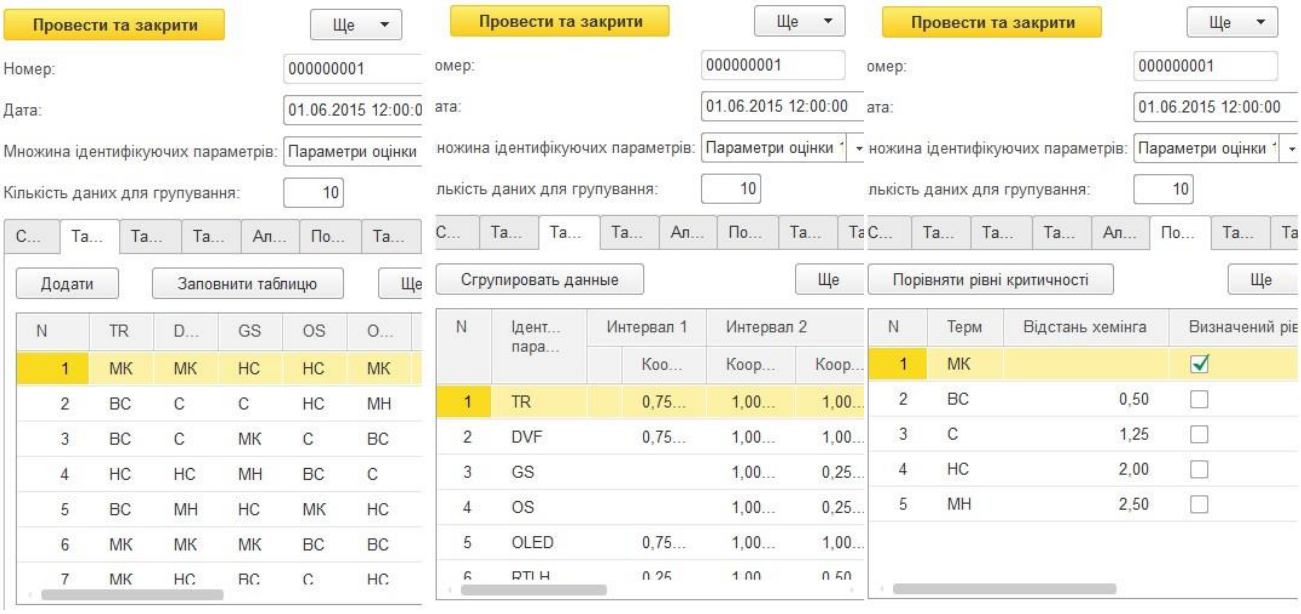

Рис. 15. Вікно форми елемента документа «Оцінка рівня критичності»

Таким чином, можна побачити, що структура ПЗ *«СОКС v.1.0»* дуже подібна до попередньої програмної розробки, а інтерфейс практично ідентичний в аспекті інструментарію побудови нечітких чисел, лінгвістичних змінних та термів. Функціонал обох розроблених програмних рішень дозволяє їх використовувати за прямим призначення запропонованого комплексу, а також використовувати його для моделювання його роботи під час експериментальних досліджень. Проведені експерименти будуть висвітлені в наступних роботах.

Висновки

На основі запропонованих моделей, методів та нових структурних рішень розроблено програмний комплекс для управління кризовими ситуаціями, який дозволяє автоматизувати ці процеси за рахунок побудови лінгвістих змінних та термів кожного параметру, наборів евристичних правил та проведення арифметичних дій, в тому числі нечітких, безпосередньо на програмному рівні.

Так, на основі методу виявлення інцидентів/потенційних кризових ситуацій та структури системи виявлення інцидентів/потенційних кризових ситуацій розроблений програмний засіб *«СВІПКС v.1.0»* в розробницькому середовищі 1С Підприємство 8.3. До складу програмного забезпечення входять об'єкти типу «Довідники» («Множина ідентифікуючих параметрів», «Ідентифікуючі параметри», «Терми лінгвістичних змінних», «Інтервали», «Види ІПКС», «Лінгвістичні ідентифікатори можливості реалізації ІПКС») та «Документи» («Формування еталонів», «Набори евристичних правил», «Оцінка поточного стану середовища»). В ньому реалізується процеси виявлення інцидентів, що потенційно здатні спровокувати кризові ситуації в інформаційній сфері.

А на основі методу оцінки критичності ситуацій та структури системи оцінки критичності ситуації розроблений програмний засіб *«СВОКС v.1.0»* в розробницькому середовищі 1С Підприємство 8.3. До складу програмного забезпечення входять об'єкти типу «Довідники» («Множина оціночних параметрів», «Оціночні параметри», «Терми лінгвістичних змінних» та «Інтервали») та «Документи» («Еталони», «Оцінка рівня критичності»). В ньому реалізується процеси обрахунку показника рівня критичності поточної ситуації та створення індикатора рівня критичності, що відображає динаміку розвитку кризової ситуацій, що виникла в інформаційній системі.

Зазначені результати впроваджені у діяльність ТОВ «Сайфер ЛТД», ТОВ «Hazon», Національного авіаційного університету. Крім того, таке програмне забезпечення може бути складовою частиною комплексної системи захисту інформації будь-якого підприємства та особливо корисне для команд реагування на комп'ютерні та кіберінциденти, зокрема здатністю роботи в режимі реального часу.

Література

[1] EM–DAT: The OFDA/CRED International Disaster Database». Brussels, Belgium. URL: http://www. em–dat.net.

[2] С.А. Петренко, А.В. Беляєв, «Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться». М.: ДМК–Пресс. Компания АйТи. 2011. 400 с.

[3] Б.Д. Альтерман, В.И. Дрожжинов, Г.Е. Моисеенко. «Обеспечение непрерывности деятельности организации в нештатных ситуациях». *Jet Info*. №5(120). 2003. 28 с.

[4] S. Harris. «CISSP Certification All–in–One Exam Guide». *McGraw–Hill Osborne Media*. 7th Edition. 2016. 1431 p.

[5] А.Б. Качинський. «Безпека, загрози і ризик: наукові концепції та математичні методи». К.: Нац. акад. служби безпеки України. 2004. 471 с.

[6] А.І. Гізун, І.Л. Лозова. «Аналіз дефініцій поняття кризова ситуація та основних аспектів концепції управління безперервністю бізнесу». *Безпека інформації*. Т.22. №1. 2017. С. 99-108.

[7] А.Г. Корченко. «Построение систем защиты информации на нечетких множествах. Теория и практические решения». К.: МК–Пресс. 2006. 320 с.

[8] М.П. Карпінський, А.О. Корченко, А.І. Гізун. «Метод виявлення інцидентів/потенційних кризових ситуацій». *Захист інформації*. Т.17. №2. 2015. С. 124-130.

[9] А.О. Корченко, В.А. Козачок, А.І. Гізун. «Метод оцінки рівня критичності для систем управління кризовими ситуаціями». *Захист інформації*. Т.17. №1. 2015. С. 86-98.

[10] М.П. Карпінський, А.О. Корченко, А.І. Гізун. «Інтегрована модель представлення кризових ситуацій та формалізована процедура побудови еталонів ідентифікуючих параметрів». *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. В.1 (29). 2015. С. 76-85.

[11] А.І. Гізун. «Обчислювальний комплекс виявлення та оцінювання кризових ситуацій в інформаційній сфері». *Захист інформації*. Т.18. №1. 2016. С. 66-73.

[12] Огляд нової платформи «1С Підприємство 8.3». URL: http://erp-project.com.ua/index.php/uk/novini/item/206-obzor-novojplatformy-1s-predpriyatie-8-3.

УДК 004.056.53:004.492.3 (045)

Гизун А.И. Программный комплекс обнаружения и оценки кризисных ситуаций в информационной сфере

Аннотация. *Обеспечение устойчивого развития человечества и его безопасности аспектов на сегодня тесно связано с необходимостью управления инцидентами/потенциальными кризисными ситуациями. В частности, важно их своевременное выявление, идентификация и оценка. Так, возникновение различного рода инцидентов информационной безопасности могут серьезно повлиять на бизнес-процессы любого предприятия, а при достижении уровня их влияния на информационную систему определенного критического значения возникает возможность появления кризисной ситуации. Особое направление стратегического менеджмента, который регулирует процессы управления кризисными ситуациями - их выявление, идентификацию, оценку, нейтрализацию, предупреждение и ликвидацию последствий - управление непрерывностью бизнеса берет свое начало еще в 80-тх годах прошлого столетия. Однако еще недавно в этой сфере преобладали системы, основными функциями которых были только поддержка информационных технологий в условиях кризиса, нейтрализация или ликвидация последствий, документационное обеспечение формирования и выполнения планов непрерывности бизнеса. И только сейчас внимание начали акцентировать на процедуре раннего выявления кризисной ситуации или оценки ее деструктивного влияния. Современные системы управления кризисными ситуациями в большинстве используют математические модели, основанные на теории вероятностей, признаковых и компараторных моделях, имеют ряд существенных недостатков. В работе предлагается вниманию программное обеспечение, которое реализует разработанный вычислительный комплекс обнаружения и оценки кризисных ситуаций в информационной сфере, работа которого основывается на использовании нечетких слабоформализованих моделей и методов с применением экспертных подходов. Такой комплекс позволяет нивелировать основные недостатки известных подобных решений, в том числе зависимость от статистических данных, скорости их обработки, неполноты и нечеткости исходных данных. В данной статье описана программная реализация вычислительного комплекса обнаружения и оценки кризисных ситуаций в информационной сфере, его интерфейс и функционал, описаны режимы работы и особенности применения как в режиме реального времени, так и для моделирования кризисных ситуаций различного рода.*

Ключевые слова: *кризисная ситуация, метод, система, концепция управления непрерывностью бизнеса, нечеткая логика, программное обеспечение, интерфейс, функционал, программный модуль.*

Gizun A. The software complex for the detection and evaluation of crisis situations in the information field

Abstract. *Ensuring the sustainable development of mankind and its safety aspects is closely related to the necessity of incidents/potential crisis situations governance. Particularly, the most significant aspect is timely identification, identification and evaluation different incident. Thus, the emergence of different information security incidents can seriously affect the business processes in enterprise, and, when a certain critical level of their influence on the information system is reached, a crisis situation is emergence. A special area of strategic management, which regulates the crisis management processes-their identification, identification, assessment, neutralization, prevention and liquidation of consequences – business continuity management dates back to the 80s of the last century. However, until recently, systems, the main functions of which were information technologies support in crisis conditions, neutralization or elimination of consequences, documentation support for the formation and implementation of business continuity plans had dominated in this sphere. And only now, attention on the procedure for early detection of crisis situations or an assessment of its destructive influence is focused. The modern crisis management systems mostly use mathematical models which based on probability theory, indicative and comparator models, and have a number of significant weaknesses. In the paper offers the software complex that implements the developed computer complex for the detection and evaluation of crisis situations in the information field, its work is based on the use of fuzzy weakly formalized models and methods using of expert approaches. Such complex allows to level out the main weakness of known similar solutions, including dependence on statistical data, speed of their processing, incompleteness and unclear initial data. In this paper describes the software implementation of the computer complex for detection and evaluation of crisis situations in the information field, its interface and functional, describes the operation modes and application features both in real time mode and for modeling various types of crisis situations.*

Key words: *crisis situation, method, system, business continuity management concept, fuzzy logic, software, interface, functional, software module.*

Отримано 18 *червня 2017 року*, затверджено редколегією 6 *липня 2017 року*