ВІДГУК

офіційного опонента Кудіна Антона Михайловича

на дисертацію Гізуна Андрія Івановича «Методи та засоби оцінювання параметрів безпеки для виявлення кризових ситуацій в інформаційній сфері», представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації»

Актуальність. Постійний розвиток людського суспільства характеризується ростом залежності практично всіх процесів управлінської діяльності від інформаційних технологій з одного боку та збільшенням числа і складності інцидентів IT-безпеки, які можуть переривати бізнес-процеси та навіть ставити під загрозу успішне функціонування самих підприємств, установ і організацій всіх форм власності. Залежно від масштабу, частоти та інших характеристик інциденти IT- безпеки можуть набувати нової сутності – кризових ситуацій, вплив яких має значно суттєвіші наслідки на загальну IT інфраструктуру організації. Забезпечення безперервності функціонування інформаційно-комунікаційних систем на сьогодні регулюється рядом міжнародних стандартів та специфікацій (ISO 22301:2012, ISO 22313:2012, BS 25999 і інші), реалізується у відповідності з кращими світовими практиками (BSI, DRII, Gartner, HP та інші) і безумовно є важливим напрямом IT-безпеки. У відповідності з керівними документами даної галузі своєчасне виявлення та ідентифікація інцидентів чи кризових ситуацій, що загрожують організації, і підбір адекватних їх рівню контрзаходів, що є можливим лише після процесу оцінки критичності ситуації, дозволяє мінімізувати негативних наслідки для інформаційно-комунікаційних систем і організацій взагалі. Таким чином ефективне управління кризовими ситуаціями, що вміщує етапи виявлення, ідентифікації, оцінки кризових ситуацій, реагування та ліквідації їх наслідків, які і висвітлені та реалізовані на основі нечіткої логіки в дисертаційній роботі Гізуна А.І., є важливою науковою задачею, а дослідженням з цього приводу приділяється значна увага в усьому світі.

Більшість з відомих систем управління кризовими ситуаціями використовує апарат звичайної логіки, сигнатурні і статистичні методи, а також теорію ймовірностей, що не дає змоги забезпечити належну ефективність їх функціонування в нечітких умовах в слабоформалізованому середовищі, і вимагають значних витрат часових і виробничих ресурсів та пов'язані з необхідністю формування статистичних даних, процесами

навчання систем тощо. Застосування апарату нечіткої логіки та експертних методів дає можливість суттєво усунути зазначені обмеження.

Одержані результати дисертаційної роботи відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету («Нові методи і моделі систем виявлення кібертерористичних атак», № 0108U004007, «Організація систем захисту інформації від кібератак», № 0111U000171).

Таким чином, усе сказане обумовлює актуальність дисертаційної роботи Гізуна А.І. і наукову новизну поставлених в ній задач досліджень.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Викладені наукові положення, висновки і рекомендації є повністю обґрунтованими, а достовірність теоретичних положень підтверджується коректним застосуванням відомого математичного апарату, експериментальними даними та результатами верифікації запропонованих моделей та методів, а також впровадженням в практику.

Структура дисертації

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків щодо основних результатів роботи, списку використаних джерел та додатків.

У **вступі** автором представлена загальна характеристика роботи, обґрунтована актуальність, сформульовані мета і задачі досліджень, відображені наукова новизна і практична цінність отриманих результатів, наведено дані про їх апробації та впровадження.

У **першому розділі** проведено детальний аналіз сучасного стану теоретичної та практичної бази, методів та засобів управління кризовими ситуаціями в аспекті забезпечення безперервності бізнесу загалом та роботи інформаційно-комунікаційних систем зокрема. Визначено місце процесів управління кризовими ситуаціями в менеджменті інформаційної безпеки, що відповідає основним положенням стандартів і специфікацій, в тому числі і серії ISO 27000. Проведене дослідження вітчизняних та міжнародних розробок в галузі управління кризовими ситуаціями, а саме: систем раннього виявлення кризових ситуацій, методів і засобів прогнозування кризових ситуацій, систем та апаратів зменшення збитків та формування планів діяльності в умовах непередбачуваних ситуацій. У результаті багатокритеріального аналізу встановлено, що усі ці засоби не є досконалими і мають певні обмеження щодо їх практичного застосування. Частина першого розділу присвячена питанню підходів до класифікації кризових ситуацій та періодизації процесів кризового управління.

Встановлено, що на сьогодні немає єдиної класифікації, що змогла б охопити всі необхідні характеристики для прогнозування та виявлення кризових ситуацій. Даний факт підкреслює актуальність створення узагальненої класифікації та таксономії.

У **другому розділі** розроблено узагальнену класифікацію кризових ситуацій, що носить ознаковий принцип і диференціює кризові ситуації за такими базовими характеристиками як: причина походження подій (джерело), що може зумовити виникнення кризової ситуації; можливість прогнозування; ступінь прояву; масштаб прояву кризової ситуації (в географічному та організаційному аспекті); глибина вияву кризових явищ; характер виникнення; час дії негативних чинників кризової ситуації; потенційна загроза людському життю та здоров'ю; кількість жертв; рівень економічних збитків. В подальшому класифікація використана для побудови моделей та методів управління кризовими ситуаціями, зокрема для оцінки критичності ситуації, породженої інцидентами інформаційної безпеки. Розроблена модель представлення інцидентів інформаційної безпеки - потенційних кризових ситуацій, яка формується шестикомпонентним кортежем. Кортеж вміщує такі компоненти як: ідентифікатор інцидентів, підмножини можливих параметрів, нечітких лінгвістичних еталонів, поточних значень параметрів, евристичних правил і показник рівня критичності ситуації. Запропонована інтегрована модель дозволяє формалізувати процес виявлення інцидентів або кризових ситуацій (залежно від їх рівня критичності) в нечіткому слабоформалізованому середовищі. Крім того описані і формалізовані процеси формування еталонів нечітких параметрів та евристичних правил.

У **третьому розділі** розроблено два методи управління кризовими ситуаціями, а саме: метод виявлення інцидентів/потенційних кризових ситуацій та метод оцінки критичності ситуації, на основі яких запропоновані архітектури системних рішень для розширення функціональних можливостей сучасних систем прогнозування, виявлення, ідентифікації та оцінки кризових ситуацій. В основі даних методів лежать інтегрована модель представлення кризових ситуацій та теорії нечітких множин Заде, адаптованої до вирішення задач інформаційної безпеки, методах нечіткої логіки (лінгвістичних термів з використанням статистичних даних (МЛТС) – для побудови еталонних значень параметрів та оціночних еталонів; лінійної апроксимації по локальним максимумам (ЛАЛМ) – для виконання нечітких математичних операцій; узагальненої відстані Хемінга (УВХ) – для порівняння поточних і еталонних значень параметрів) і методах експертного оцінювання (середніх рангів (СР) та

попарного порівняння з визначенням квадратного кореня (ППВКК)). На відмінну від існуючих методів та систем управління кризовими ситуаціями запропоновані рішення можуть ефективно працювати в нечіткому слабоформалізованому середовищі, не вимагають обробки статистичних даних, можуть виявляти раніше невідомі інциденти за евристичним принципом.

Четвертий розділ присвячено практичним реалізаціям та експериментальним дослідженням запропонованих рішень. Розроблено методику проведення експериментального дослідження, в якій визначено мету та задачі експерименту, вхідні та вихідні параметри, гіпотезу і критерії дослідження, а також послідовність необхідних дій. Для проведення експерименту, на основі описаних в розділах 2 і 3 моделей та методів і в відповідності з запропонованою структурою систем розроблено програмне забезпечення «СВІПКС v.1.0» та «СОКС v.1.0», які реалізують виявлення інцидентів та оцінювання рівня критичності ситуації, спричиненої виявленим інцидентом, що проілюстровано на конкретних прикладах. Результати проведених експериментів підтвердили адекватність, точність та достовірність наукових положень та практичних рішень, запропонованих автором.

У висновках стисло сформульовано основні наукові та практичні результати дисертаційної роботи.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи та фрагменти вихідних текстів програм, що відображають практичну частину дисертаційного дослідження, а також множини евристичних правил, за якими здійснюється виявлення інцидентів в інформаційних системах, наведені у вигляді таблиць.

Наукова новизна отриманих результатів дисертаційної роботи полягає у наступному:

– вперше розроблена інтегрована модель представлення інцидентів/потенційних кризових ситуацій, що за рахунок інтегрування ідентифікаторів інцидентів, підмножин можливих параметрів, нечітких лінгвістичних еталонів, поточних значень параметрів, евристичних правил і показника рівня критичності ситуації в шестикомпонентному кортежі, дозволяє сформувати базові оціночні та ідентифікуючі компоненти для відображення процесу виявлення кризових ситуацій;

– вперше розроблені метод виявлення інцидентів/потенційних кризових ситуацій та метод оцінки критичності ситуації, що за рахунок обробки нечітких ідентифікуючих та оціночних параметрів, використання інтегрованої моделі представлення інциденту, моделей еталонів та

евристичних правил, а також множин формування індикатора рівня критичності, який дозволяє виявити інциденти/потенційні кризові ситуації та оцінити критичність ситуації, що склалася внаслідок впливу зазначених інцидентів;

– вперше розроблені структурні рішення систем управління кризовими ситуаціями, які за допомогою зазначених в дисертаційні роботі структурних блоків дозволяють створити системи управління кризовими ситуаціями, які функціонують в нечіткому середовищі;

– отримали подальший розвиток модель евристичних правил, в якій за рахунок апарату логічних зв'язок, лінгвістичних ідентифікаторів та унікальних ідентифікаторів поточних станів, формуються множини необхідних евристичних правил.

Публікації та апробація. Основні положення дисертації опубліковано у 19 наукових працях, у тому числі 12 статей у фахових наукових виданнях (11 з яких входять до міжнародних наукометричних баз), 1 стаття у збірнику наукових праць та 6 тез доповідей і матеріалів конференцій, що повністю задовольняє чинним вимогам МОН України до дисертацій наукового ступеня кандидата наук. Зазначені положення дисертаційної роботи пройшли обов'язкову апробацію на численних науково-технічних конференціях та семінарах.

Відповідність змісту автореферата дисертації. Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі і задовольняє встановленим вимогам.

Значення результатів для науки та практична корисність роботи. Цінність дисертації полягає в тому, що в ній запропоновано рішення важливої науково-технічної задачі розширення можливостей системи управління кризовими ситуаціями в ІТ сфері. Практична корисність роботи обумовлена тим, що використання запропонованих в ній формальних методів і конкретних рішень дозволяє проектувати більш досконалі, порівняно з відомими, програмні та програмно-апаратні засоби виявлення та оцінки інцидентів ІТ-безпеки – потенційних кризових ситуацій. Запропоновані методи і моделі використані при розробці спеціального програмного забезпечення для виявлення інцидентів/потенційних кризових ситуацій та оцінки критичності ситуації, що підтверджується актами впровадження у діяльність ТОВ «Сайфер ЛТД», розроблені комп'ютерні програми «Система виявлення ІПКС» та «Система оцінки критичності ситуації» використовується в навчальному процесі підготовки фахівців у галузі знань 1701 «Інформаційна безпека» для ідентифікації і виявлення інцидентів різного характеру в нечітких слабоформалізованих середовищах

для підтримки прийняття рішень в умовах дії кризових ситуацій. Дані результати підтверджені актами впровадження у діяльність ТОВ «Hazon» та навчальний процес Національного авіаційного університету. Крім того розроблено методику експерименту для дослідження запропонованих засобів виявлення, ідентифікації та оцінки кризових ситуацій.

Зауваження

1. В першому розділі не достатньо уваги приділено питанням співвідношення методів, запропонованих автором та відомим методикам детального аналізу ризиків. Було б доцільно більш точно підкреслити відмінності між цими напрямами наукових досліджень.

2. Термінологія, яка використовується автором іноді не співпадає із загальновживаною в теорії захисту інформації.

3. При побудові узагальненої класифікації кризових ситуацій не зовсім зрозуміло з яких саме позицій вибрані базові характеристики і чи враховані при її побудові відомі класифікації загроз інформаційній безпеці, зокрема – класифікація CVE.

4. В описі системи виявлення інцидентів/потенційних кризових ситуацій в розділі 3 відзначено, що до її складу входить «…регістри ІПКС (РІПКС). … В РІПКС заносяться ідентифікатори основних класів інцидентів…». Враховуючи те, що у регістрах зберігаються не інциденти, а їх ідентифікатори, то цей регістр було б коректніше назвати регістром ідентифікаторів інцидентів/потенційних кризових ситуацій (РІІПКС).

5. Розробка евристичних правил передбачає участь експертів з питань захисту інформації в інформаційно-комунікаційних системах. У багатьох прикладах обчислень, наведених у дисертаційній роботі, використовуються результати експертних оцінювань. Однак відсутня інформація про самих експертів (їх досвід, рівень кваліфікації та ін.). Можливо доцільно було б приділити більше уваги розгляду питань залежності отриманих результатів від рівня компетентності експертів та узгодженості експертних оцінок.

6. З роботи не зовсім зрозуміло яким чином одержані вихідні дані для системи оцінки критичності ситуації під час проведення експериментальних досліджень.

7. Назви етапів методів виявлення інцидентів/потенційних кризових ситуацій та оцінки критичності ситуації в тексті дисертаційної роботи та на рис.3.1 (ст. 109) і 3.2 (ст. 114) дещо різняться між собою. Крім того, в методі оцінки критичності ситуації, етапи 2.1. – «Формування множини оціночних параметрів» та 2.3 – «Обчислення коефіцієнтів важливості (КВ) і ранжування оціночних параметрів» варто об'єднати в один з назвою «Формування та обробка вихідних і експертних даних».

8. В дисертації не проведено порівняльний аналіз технічних показників запропонованих розробок з існуючими рішеннями. Якщо, на думку автора, в даний час відсутні аналогічні системи виявлення кризових ситуацій на основі експертного підходу та аналізу нечітких даних, слід було б явно на це вказати.

ВИСНОВКИ

У цілому дисертаційна робота Гізуна А.І. є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для розвитку теорії й практики управління кризовими ситуаціями: їх виявлення, ідентифікації, оцінювання та нейтралізації, що у подальшому можуть використовуватися для підвищення ефективності сучасних систем захисту інформації. Одержані наукові результати можуть також застосовуватися в інших галузях науки і техніки, де необхідно розв'язувати задачі пов'язані з прийняттям рішень в умовах невизначеності та впливу кризових ситуацій, забезпеченні технологічної безпеки виробництва тощо.

Вважаю, що дисертаційна робота «Методи та засоби оцінювання параметрів безпеки для виявлення кризових ситуацій в інформаційній сфері» **повністю відповідає вимогам МОН України,** зокрема п. 9, 11, 12 Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника від 24 липня 2013 р. № 567, а її автор Гізун Андрій Іванович **заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».**

ОФІЦІЙНИЙ ОПОНЕНТ

Начальник управління Служби безпеки України,
доктор технічних наук, старший науковий співробітник

А.М. Кудін

15 вересня 2015 р.

Підпис Кудіна А.М. засвідчую
Заступник керівника кадрового підрозділу СБ України

Ю.В. Матвійчук

15 вересня 2015 р.