ВІДГУК

офіційного опонента Браіловського Миколи Миколайовича

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. Рецензована дисертаційна робота спрямована на вирішення важливої науково-технічної задачі розвитку систем управління кризовими ситуаціями, що функціонують за принципом виявлення аномалій на основі методів нечіткої логіки.

Використання сучасних комп'ютерних технологій у всіх сферах діяльності суспільства дозволило здійснювати автоматизовану обробку великих об'ємів даних. Але разом з цим зросла залежність функціонування підприємств, установ та організацій від безперервності роботи інформаційних систем, яка досить часто може перериватися інцидентами різного роду та кризовими ситуаціями. Таке становище негативно впливає на стан безпеки ресурсів інформаційних систем внаслідок непередбачуваності появи кризових ситуацій, їх значного впливу на сучасні бізнес-процеси.

Тому однією з важливих наукових проблем в області інформаційного захисту на сьогоднішній день є напрям, пов'язаний з ідентифікацією, виявленням, прогнозуванням інцидентів інформаційної безпеки, що за певних умов можуть перерости в кризові ситуації, а також з оцінюванням критичності загрози інформаційним ресурсам, що виникають під впливом надзвичайних ситуацій, в тому числі і в інформаційній сфері. Одним із поширених рішень цієї проблеми є системи управління кризовими ситуаціями, які на сьогодні практично відсутні в сфері забезпечення інформаційної безпеки. Системи управління кризовими ситуаціями (які можуть базуватися як на програмних, так і на апаратно-програмних засобах) в залежності від застосованого методу аналізу подій можна поділити на два загальні класи: ті, що використовують сигнатури, та ті, що виявляють аномалії, породжені атакуючими діями.

Головною перевагою систем, що виявляють аномалії, є здатність виявляти нові, невідомі раніше типи інцидентів, зокрема, на ранніх стадіях їх розвитку. До недоліків систем на базі виявлення аномального стану відноситься потреба у складних і тривалих підготовчих процедурах, пов'язаних з отриманням статистичних даних та реалізацією процесу навчання системи. Усунути ці недоліки здатні підходи, засновані на використанні

досвіду експертів, але при реалізації таких рішень необхідно обробляти дані, що подаються в нечіткій (лінгвістичній) формі. Формалізувати таку інформацію і провести її обробку дозволяє теорія нечітких множин. Тому розроблення моделей, методів і систем виявлення кризових ситуацій в нечітких умовах є важливою науковою задачею.

В цьому зв'язку тема дисертаційної роботи Гізуна А.І. є актуальною, а розв'язання питань та задач, що в ній сформульовані, має теоретичне і прикладне значення для розробки засобів захисту інформації в комп'ютерних системах та мережах.

Результати, одержані в рецензованій дисертаційній роботі відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету та відповідних актах впровадження.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційні дослідження виконувались відповідно до планів науково-дослідних робіт Національного авіаційного університету в рамках держбюджетних наукових тем, в яких автор був співвиконавцем («Нові методи і моделі систем виявлення кібертерористичних атак», № 0108U004007, «Організація систем захисту інформації від кібератак», № 0111U000171)

Оцінка змісту дисертації, її завершеності

Викладені наукові положення, висновки і рекомендації є повністю обґрунтованими, а достовірність теоретичних положень підтверджується експериментальними даними та результатами верифікації запропонованих моделей та методів. Дані, отримані під час експериментів, відповідають теоретичним висновкам роботи і повністю підтверджують їх.

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 дефініції «кризова ситуація» та суміжних понять, розглянуті основні теоретичні положення концепції управління безперервності бізнесу, в тому числі і в інформаційній сфері. Досліджені також основні підходи до класифікації кризових ситуацій, виділені найбільш важливі принципи їх побудови. Показані стан розвитку прикладних рішень щодо прогнозування, виявлення, ідентифікації кризових ситуацій в різних сферах економіки та суспільного життя, на основі чого доведена відсутні універсальні системи управління кризовими ситуаціями, що можуть використовуватися в менеджменті інформаційної безпеки та функціонувати в умовах невизначеності.

У **другому розділі** розроблено узагальнену класифікацію кризових ситуацій, базовими характеристиками в якій є: 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. А також розроблена модель представлення інцидентів/ потенційних кризових ситуацій, у вигляді шестикомпонентного кортежу з такими елементами: ідентифікатор інцидентів, підмножина можливих параметрів, підмножина нечітких лінгвістичних еталонів, підмножина поточних значень параметрів, підмножина евристичних правил і показник рівня критичності ситуації. Запропонована інтегрована модель дозволяє формалізувати процес виявлення інцидентів/потенційних кризових ситуацій в нечіткому слабоформалізованому середовищі. Згідно запропонованої моделі під час представлення інцидентів особлива увага приділяється нечітким еталонам лінгвістичних змінних ідентифікуючих параметрів та евристичним правилам, процеси побудови яких формалізовані в підрозділі 2.2 дисертаційної роботи.

У **третьому розділі** розроблено два методи управління кризовими ситуаціями, а саме метод виявлення інцидентів/потенційних кризових ситуацій (складається з 6 етапів: етап 1.1 – формування множин ІПКС та ідентифікуючих параметрів; етап 1.2 – формування зв'язки ІПКС з параметрами; етап 1.3 – формування еталонів нечітких параметрів; етап 1.4 – формування множини евристичних правил; етап 1.5 – фазифікація параметрів, що моніторяться з метою виявлення ІПКС; етап 1.6 – обробка поточних значень ідентифікуючих параметрів і формування результату) та метод оцінки критичності ситуації (містить 6 етапів: етап 2.1 – формування множини оціночних параметрів, етап 2.2 – формування лінгвістичних змін для оцінки заданих параметрів та оціночних еталонів, етап 2.3 – обчислення коефіцієнтів важливості і ранжування оціночних параметрів, етап 2.4 – фазифікація параметрів оцінки рівня критичності, етап 2.5 – обчислення загального рівня критичності, етап 2.6 – формування індикатора критичності кризової ситуації), на основі яких запропоновані архітектури системних рішень для розширення функціональних можливостей сучасних систем прогнозування, виявлення, ідентифікації та оцінки кризових ситуацій. За рахунок використання теорії нечітких множин та експертних підходів запропоновані методи та системні рішення дають принципову можливість використовувати

їх в нечіткому слабоформалізованому середовищі, не вимагаючи обробки статистичних даних.

У **четвертому розділі** 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, необхідне інструментальне та програмне забезпечення. Експериментальні дослідження проведенні за допомогою розробленого програмного забезпечення «Система виявлення та ідентифікація ІПКС» та «Система оцінки критичності ситуації», які реалізують виявлення інцидентів та оцінювання рівня критичності поточної ситуації. Дослідження впливу значень параметрів на отримані результати щодо виявлення ІПКС підтвердили адекватність реагування системи на їх зміну, а отриманий результат роботи системи оцінки критичності ситуації підтвердив адекватність розроблених еталонів і коректність вибору множини оціночних параметрів.

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

У **додатках** вміщено акти впровадження результатів дисертаційної роботи та фрагменти кодів програм, що відображають практичну частину дисертаційного дослідження, а також у табличній формі множини евристичних правил.

Текст дисертації викладено грамотною технічною мовою логічно і послідовно. Стиль викладення доказовий. В цілому дисертація є закінченою науковою роботою, що відповідає паспорту спеціальності 05.13.21 – "Системи захисту інформації".

Найбільш суттєві результати дисертації. Наукова новизна отриманих результатів дисертаційної роботи, на мою думку, перш за все, полягає у наступному:

– розроблена узагальнена класифікація кризових ситуацій та на її основі інтегрована модель представлення інцидентів/ потенційних кризових ситуацій, в якій за рахунок інтегрування ідентифікаторів інцидентів, підмножин можливих параметрів, нечітких лінгвістичних еталонів, поточних значень параметрів, евристичних правил і показника рівня критичності ситуації в шестикомпонентному кортежі шляхом формування базових оціночних та ідентифікуючих компонентів здійснюється відображення процесу виявлення кризових ситуацій;

– отримали подальший розвиток модель евристичних правил, в якій за рахунок логічних зв'язок між введеними множинами ідентифікуючих параметрів та лінгвістичних ідентифікаторів формуються множини

необхідних евристичних правил для систем управління кризовими ситуаціями;

– розроблені метод виявлення інцидентів/потенційних кризових ситуацій та метод оцінки критичності ситуації, що за рахунок обробки нечітких ідентифікуючих та оціночних параметрів з використання інтегрованої моделі представлення інциденту, а також множин формування індикатора рівня критичності, дозволяють виявити інциденти/ потенційні кризові ситуації та оцінити критичність поточної ситуації;

– вперше розроблені структурні рішення систем управління кризовими ситуаціями, які за допомогою блоків фазифікації ідентифікуючих параметрів, формування множин фазифікованих параметрів та ідентифікатора поточного стану, блоків визначення коефіцієнтів важливості, лічильника сенсорів параметрів, фазифікації оціночних параметрів, обрахунку показника рівня критичності і блоку дефазифікації результатів, дозволяють створити системи управління кризовими ситуаціями, які функціонують в нечіткому середовищі.

Ступінь обґрунтування наукових положень, висновків і рекомендацій.

Високий рівень обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації обумовлюється строгістю використання математичний апарату та коректністю застосування методів дослідження (формування функцій належності, порівняння функцій належності, нечіткої арифметики, визначення коефіцієнтів важливості), включаючи теорію нечіткості.

Достовірність результатів теоретичних викладень, що відображені автором в запропонованих моделях, методу та структурних рішеннях, перевірені експериментально за допомогою розроблених програмних засобів. Всі результати, отримані експериментальним шляхом за допомогою практичного використання програмних розробок співпадають з теоретичними та підтверджують їх.

Оцінка висновків здобувача щодо значущості його праці для науки й практики.

Наукова значимість результатів дисертаційної роботи полягає у тому, що створені модель, методи, структурні рішення та програмне забезпечення вирішують наукову задачу виявлення кризових ситуацій інформаційної сфери умовах нечіткості. Практична цінність результатів роботи полягає в тому, що вони можуть застосовуватись при створенні засобів захисту інформації у вигляді програмних або апаратно-програмних модулів, що дає змогу підвищити ступінь захищеності комп'ютерних систем та мереж. На основі запропонованих методів розроблено відповідне програмне забезпечення для

виявлення та оцінювання кризових ситуацій. Всі наукові положення дисертаційної роботи отримані автором самостійно, основні результати впроваджено в діяльність ТОВ «Сайфер ЛТД», ТОВ «Hazon» та навчальний процес Національного авіаційного університету.

Повнота викладу результатів досліджень в опублікованих працях.

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 чинні вимоги МОН України до кандидатських дисертацій, та пройшли обов'язкову апробацію на науково-технічних конференціях та семінарах.

Автореферат дисертації відповідає вимогам щодо його оформлення, відображає основні положення дисертаційної роботи, містить необхідні дані для її оцінки фахівцями.

Відповідність теми та змісту дисертації паспорту спеціальності, за якою вона подана на захист.

Тема дисертації та її зміст відповідають формулі й галузі досліджень паспорта спеціальності 05.13.21 – "Системи захисту інформації", оформлена відповідно до вимог значних стандартів.

Недоліки та зауваження по роботі.

1. В розділі 1.2 дисертаційної роботи автором розглянуті сучасні системи, що застосовуються для задач, пов'язаних з плануванням безперервності бізнесу, що мають опосередкований зв'язок з отриманими результатами. На мій погляд, доцільно було б замість цього більш детально розглянути системи та засоби, що застосовуються для виявлення та попередження вторгнень в інформаційні системи та мережі, для оцінки ризиків тощо.

2. В таблиці 1.4 дисертаційної роботи наведено порівняння сучасних систем управління кризовими ситуаціями за низкою критеріїв. Однак відсутнє пояснення до них, що ускладнює розуміння результатів аналітичного дослідження.

3. При застосуванні експертного підходу для формування еталонів та евристичних правил автор не враховує такі чинники, як погодженість суджень експертів та рівень їх компетентності.

4. В розділі 2 дисертаційної роботи автор описує множини евристичних правил в словесній формі та у вигляді математичного опису як формула (2.11). На мою думку, достатньо лише математичного опису даної множини правил. Крім того самі правила в роботі називаються то «евристичними», то «вирішальними» - слід було б узгодити даний момент.

5. В роботі не зрозуміло з яких позицій автором здійснений вибір досліджуваних класів інцидентів/потенційних кризових ситуацій та використовуваних ідентифікуючих та оціночних параметрів.

6. Ускладнене розуміння зображень структури розроблених систем на рисунках 3.6 та 3.7 дисертаційної роботи внаслідок використання великої кількості абревіатур та формул.

ВИСНОВКИ

Дисертаційна робота Гізуна Андрія Івановича «Методи та засоби оцінювання параметрів безпеки для виявлення кризових ситуацій в інформаційній сфері» є самостійною завершеною науковою роботою. В дисертації отримані нові науково обґрунтовані результати, які вирішують науково-практичну задачу виявлення та ідентифікації кризових ситуацій та оцінки рівня загрози інформаційним ресурсам, спричиненої ними, що в сукупності є значним досягненням для розвитку систем захисту інформації.

Матеріал дисертації викладено послідовно, стиль викладання доказовий, чіткий і лаконічний. Висновки до кожного розділу і дисертації в цілому тісно пов'язані з їх змістом і відображають суть виконаних досліджень. Публікації автора повністю висвітлюють наукові положення і результати дисертації.

Таким чином дисертаційна робота відповідає вимогам пунктів "Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника", затвердженого Постановою Кабінету Міністрів України №567 від 24 липня 2013 р., а її автор Гізун Андрій Іванович заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – "Системи захисту інформації"

ОФІЦІЙНИЙ ОПОНЕНТ

завідуючий кафедрою «Комп'ютерних систем та мереж»

Державного університету телекомунікацій

к.т.н., доцент **М.М. Браіловський**

Підпис М.М. Браіловського
засвідчую

Начальник
відділу кадрів ДУТ
С.М. Львовський