Прим. № 1

Голові спеціалізованої вченої ради Д 26.062.17
03680, м. Київ, просп. Космонавта Комарова, 1

ВІДГУК
офіційного опонента

професора кафедри інформаційних технологій і математичних дисциплін Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка, доктора технічних наук, професора *БУРЯЧКА Володимира Леонідовича* на дисертаційну роботу *КАЗМІРЧУК Світлани Володимирівни* «Методологія оцінювання ризиків безпеки ресурсів інформаційних систем», подану на здобуття наукового ступеня доктора технічних наук за 05.13.21 – системи захисту інформації

1. Актуальність теми дисертації, зв'язок з науковими програмами, планами, темами.

Інтенсивний розвиток інформаційних технологій та їх інтеграція практично у всі сфери життєдіяльності суспільства і держави відкриває можливості масового доступу користувачів до інформації. Це сприяє збільшенню кількості критично важливого інформаційного ресурсу (ІР), який циркулює, накопичується та обробляється в інформаційних системах (ІС), породжує неконтрольоване зростання кількості уразливостей ресурсів власне самих ІС (РІС) від різних проявів стороннього кібернетичного впливу й, як наслідок, призводить до підвищення ступеня залежності більшості важливих рішень, що приймаються на різних рівнях, від якості ІР та оперативності його обробки, а також від ступеня захищеності РІС від ризиків безпеки.

Зважаючи на проблемну ситуацію, яка склалася, саме здатність суспільства та його інститутів збирати, накопичувати й використовувати ІР, забезпечувати своєчасний доступ до нього та свободу інформаційного обміну, а також захищати критично важливу інформацію від внутрішніх і зовнішніх загроз, стає нині важливим чинником забезпечення національної безпеки й виступає запорукою як для соціального та технологічного прогресу, так й для швидкого економічного зростання об'єктів і суб'єктів державної та позадержавної власності.

Такий стан справ призводить до того, що нині, в умовах фактичного проведення країнами світу одна проти одної інформаційних та кібервоєн, прикладом чому є потерпаюча від неприкритої гібридної війни та російської збройної агресії Україна, надзвичайно актуальною стає проблема щодо забезпечення безпеки ІС в режимі реального часу без залучення експертів відповідної предметної галузі. Її вирішення має ґрунтуватися на ефективному оцінюванні ризиків безпеки ресурсів ІС за рахунок створення відповідних методів, моделей та засобів оцінювання.

В умовах України це, за рахунок мінімізації ризиків безпеки РІС, дозволить підвищити ефективність захисту власне самого ІР, який циркулює, накопичується та обробляється в ІС. Саме цьому й присвячена дисертаційна робота *Казмірчук Світлани Володимирівни*. Зважаючи на те, що в умовах сьогодення існують протиріччя між

наявними ресурсами ІС і нормативно-правовими, організаційними та інженерно-технічними напрямками їх захисту, а система оцінюванні ризиків безпеки РІС є недосконалою – тематика дисертаційної роботи *Казмірчук С.В.* є актуальною.

2. Аналіз основного змісту, наукової новизни та практичної значимості, оцінка достовірності та обґрунтованості результатів

Дисертація складається зі вступу, п'яти розділів, висновків, двох додатків та списку використаних джерел, що містить загалом 122 найменування. Загальний обсяг дисертації становить 383 аркуші, з яких основний зміст роботи розкрито на 312 аркушах.

Зміст роботи відповідає поставленому науковому завданню та сформульованим задачам. Їх рішення є суттю та змістом виконаних досліджень, які відповідають паспорту спеціальності 05.13.21 – системи захисту інформації й спрямовані на розробку методології оцінювання ризиків безпеки РІС, орієнтованої на створення

При цьому ***у вступі*** автором обґрунтовано актуальність досліджуваної проблеми та висвітлено її поточний стан, чітко сформульовано мету, котра корелює з темою роботи, та деталізується у задачах, визначено об'єкт та предмет дослідження. Визначено систему використаних в роботі дослідницьких методів та інструментів.

У ***першому розділі*** автором проведено аналіз світового досвіду оцінювання ризиків (ОР), а також низки відкритих баз даних (БД) уразливостей. За його результатами автором:

1) визначено, що в основному для ОР використовуються статистичні дані відносно інцидентів та загроз ІБ з урахуванням певних обмежень в аналізованих засобах;

2) констатовано, що при практичному використанні таких засобів ОР виникають ситуації, в яких для аналізу та оцінювання ризиків (АОР) доцільно застосовувати як додаткові еталони, так і еталони з іншою кількістю термів. В цьому випадку слід здійснювати їх визначення (перевизначення), для чого необхідно залучати експертів відповідної предметної галузі, що потребує значних фінансових і часових витрат та в реальних умовах є досить проблематичним

З урахуванням такого автором визначено основні задачі та напрямки наукового дослідження, що охоплюються дисертаційною роботою.

У ***другому розділі*** на основі розробленої аналітико-синтетичної кортежної моделі характеристик ризиків (АСКМ), що встановлює взаємозв'язки між множинами характеристик ризиків, підмножинами їх ідентифікуючих та оціночних компонентів, автором обґрунтовано формалізовану процедуру формування множин параметрів для ефективної організації процесу вибору існуючих інструментальних засобів і розробки відповідних методів і систем ОР, тобто процес формування необхідних характеристик ризиків.

Як результат, це дозволить підвищити ефективність прийняття рішення при виборі серед існуючих інструментальних засобів оцінювання тих, що будуть найбільш раціональними при створенні ефективної системи оцінювання ризиків ІБ.

У ***третьому розділі*** автором розроблено комплекс методів модифікації лінгвістичних змінних, що використовуються для оцінювання та управління ризиками ІБ при нечітких умовах в слабоформалізованому середовищі оточення.

За рахунок використання відповідних аналітичних функцій інкрементування і

декрементування числа термів та їх модифікацій повним n-кратним розширенням, а також базових аналітичних виразів верифікації модифікованих лінгвістичних змінних, це дозволило авторові:

по-перше, реалізувати процедуру трансформування базових еталонів параметрів на трапецієподібних і трикутних нечітких числах без залучення експертів відповідної предметної галузі;

по-друге, розширити математичну базу теорії нечітких множин (НМ), що пов'язана з операціями над лінгвістичними змінними щодо перевірки властивостей рівномірності, нерівномірності, прогресії та регресії лінгвістичних змінних до і після їх відповідного функціонального перетворення;

по-третє, забезпечити системам ОР властивість адаптивності.

У ***четвертому розділі*** автором розроблено метод перетворення інтервалів для систем аналізу та оцінювання ризиків інформаційної безпеки в нечітких числах із заданою кількістю термів. За рахунок реалізації процедур коригування параметрів, формування нових значень абсцис, визначення базового значення зсуву, поправки термів і нормування результуючих нечітких чисел це *дозволило* авторові формалізувати процес формування еталонів величин без участі експертів відповідної предметної галузі. Окрім цього автором у четвертому розділ удосконалено відомі методи оцінювання ризиків безпеки ресурсів інформаційних систем, а саме:

1) інтегрований метод оцінювання ризиків ІБ, який за рахунок формалізованого механізму формування множин параметрів, що інтегрує АСКМ і методів формування її кортежів характеристик ризиків, а також функціонально повного базису методів модифікації ЛЗ для трансформування еталонів параметрів, *дозволяє* здійснювати одночасну обробку чітких, нечітких та комбінованих величин та визначати порядок лінгвістичних величин;

2) якісно-кількісний метод ОР безпеки РІС та метод ОР безпеки РІС на основі відкритих БД загроз та уразливостей (БДЗ/У), які, за рахунок нових процедур визначення множини параметрів ОР і оцінки поточних значень параметрів з можливістю інтеграції (як альтернатива оцінок експертів) значень CVSS (Common Vulnerability Scoring System версій 2.0 та 3.0) показників у відповідних БД, формалізованого механізму формування множин параметрів, що інтегрує АСКМ і методів формування її кортежів характеристик ризиків, функціонально повного базису методів модифікації ЛЗ для трансформування еталонів параметрів, *дозволяють* здійснювати одночасну обробку чітких і нечітких та комбінованих величин з можливістю модифікації нечітких термів та автоматизувати і реалізувати в режимі реального часу відповідний процес ОР.

Автором зроблено припущення, що застосування розроблених методів найбільш доцільним буде у випадках, коли існує потреба у проведенні оцінювання ризиків ІБ як із залученням експертів, так й без їх залучення при необхідності оперативного оцінювання і моніторингу ризиків (тобто в режимі реального часу).

П'ятий розділ дисертаційної роботи присвячено розробці узагальненої методології підтримки процесів оцінювання ризиків ІБ в ІС. На підставі результатів, отриманих у попередніх розділах дисертаційної роботи, а саме за рахунок використання

формалізованого механізму формування множин параметрів, що інтегрує АСКМ і методу формування її кортежів характеристик ризиків, функціонально повного базису методів модифікації ЛЗ для трансформування еталонів параметрів, методу перетворення інтервалів, методів оцінювання ризиків безпеки ресурсів формаційних систем, авторові вдалося синтезувати системи ОР безпеки РІС з властивостями щодо адаптивності, оперативності, функціональності та надійності.

На базі запропонованої методології та структурних рішень відповідних обчислювальних систем автором розроблено алгоритмічне забезпечення для реалізації відповідного ПЗ ОР безпеки РІС, інтегровані БД і на їх основі – прикладні програмні системи ОР безпеки РІС з поліморфними властивостями, а саме ІАСОР – інтегрована адаптивна система ОР, яка використовує та динамічно визначає різні низки оціночних компонентів, що забезпечує адаптивність, надійність, функціональність її використання як в детермінованому, так і в нечіткому, слабоформалізованому середовищі без залучення експертів відповідної предметної галузі.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації, переконливо окреслена використанням сучасних методів, моделей та положень теорії захисту інформації та системного аналізу, складності систем, експертного оцінювання, методів та засобів захисту інформаційних ресурсів та ресурсів ІС тощо.

Отримані автором наукові результати у відповідності до поставлених задач досліджень є логічними, не суперечать фундаментальним фізичним і математичним закономірностям та підтверджуються достатньою апробацією основних положень і висновків як на міжнародних, так і всеукраїнських науково-технічних конференціях та семінарах.

Достовірність отриманих в роботі положень і наукових результатів підтверджується результатами проведених досліджень, коректністю застосування математичного апарату, можливих обмежень і припущень та при розробці і впровадженні нової технології побудови системи оцінювання ризиків ІС на основі засад ризик-менеджменту.

Додатково достовірність отриманих результатів експериментально підтверджується проведенням автором досліджень на науково-дослідній базі Державної служби спеціального зв'язку та захисту інформації, Національного авіаційного університету, Державної казначейської служби України тощо, що підтверджено відповідними актами впровадження.

До основних нових наукових результатів, які отримані в дисертаційній роботі, можна віднести:

1. Вперше розроблену процедуру формування множин параметрів для ефективної організації процесу вибору існуючих інструментальних засобів і розробки відповідних методів і систем оцінювання ризиків ІБ в ІС.

2. Вперше розроблений функціонально повний базис методів модифікації лінгвістичних змінних, що використовуються для оцінювання та управління ризиками ІБ при нечітких умовах в слабоформалізованому середовищі оточення;

3. Вперше розроблений метод перетворення інтервалів для систем аналізу

та оцінювання ризиків інформаційної безпеки, що використовується для формалізації процесу формування еталонів величин без участі експертів відповідної предметної галузі.

4. Удосконалені методи оцінювання ризиків безпеки ресурсів інформаційних систем, що використовуються для інтегрованої якісно-кількісної обробки різних типів початкових величин з можливістю модифікації нечітких термів та автоматизації процесу оцінювання ризиків без залучення експертів відповідної предметної галузі.

5. Вперше розроблену методологію підтримки процесів оцінювання ризиків ІБ в ІС з поліморфними властивостями щодо оцінювання ризиків безпеки їх ресурсів, що відповідає властивостям щодо адаптивності, оперативності, функціональності та надійності.

6. Вперше запропонований комплекс структурних рішень обчислювальних систем оцінювання ризиків безпеки ресурсів інформаційних систем - «РИЗИК-КАЛЬКУЛЯТОР», що реалізує розроблені/удосконалені автором методи.

Теоретична і наукова цінність та практичне значення одержаних автором наукових результатів. Як показав аналіз, результати дисертаційної роботи Казмірчук С.В. відображено у звітах НДР Державного науково-дослідного інституту спеціального зв'язку та захисту інформації України шифр «Інфраструктура», № 00114U000038д та Національного авіаційного університету (НАУ): №715-ДБ11 «Організація систем захисту інформації від кібератак», ДР № 0111U000171 (2011-2013 рр.); № 917-Х13 «Надання послуг в галузі технічного захисту інформації Головному управлінню Державної казначейської служби України у Полтавській області» (2013 р.); № 960-Х14 «Проведення державної експертизи комплексної системи захисту інформації автоматизованої системи класу «2»» (2014 р.); № 105/14.01.05 «Методологія оцінювання ризиків безпеки ресурсів інформаційних систем» (2016-2018 рр.), у яких здобувач брав участь у якості наукового керівника та відповідального виконавця.

Теоретична та наукова цінність отриманих автором результатів полягає в тому, що вони сприяють формуванню методологічного і технологічного підґрунтя для створення практичної моделі реалізації системи оцінювання ризиків безпеки в ІС.

Практичне значення отриманих результатів полягає у тому, що впровадження методології підтримки процесів оцінювання ризиків ІБ в ІС за рахунок розробленого алгоритмічного забезпечення реалізувати програмний засіб оцінювання ризиків безпеки ресурсів інформаційних систем, який дозволяє визначати різні низки оціночних компонентів, що в свою чергу забезпечує властивості адаптивності, надійності, функціональності її використання як в детермінованому, так і в нечіткому, слабоформалізованому середовищі без залучення експертів відповідної предметної галузі.

Оцінка мови та стилю викладання дисертації та автореферату. Дисертація та автореферат написані грамотно, а стиль викладення в них матеріалів досліджень, наукових положень, висновків і рекомендацій відповідає вимогам стандарту ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки» й у цілому забезпечує доступність їх сприйняття.

Зміст автореферату відображає основні результати роботи, які приведені в дисертації. Дисертація по тематиці і результатам відповідає паспорту спеціальності 05.13.21 – системи захисту інформації.

Повнота викладення наукових результатів дисертації в опублікованих роботах. Основні положення та висновки дисертаційної роботи опубліковано в 60 наукових працях. Серед них 2 монографії, 4 наукові статі у міжнародних рецензованих виданнях, що входять до баз даних Scopus та Web of Science, 6 наукових статей у закордонних фахових наукових журналах та 23 наукові статті у вітчизняних фахових наукових журналах, які входять до інших міжнародних наукометричних баз даних, а також 15 матеріалів та тез доповідей міжнародних конференцій.

Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації. Стиль викладення автореферату в цілому забезпечує його доступність та сприйняття. В ньому чітко і лаконічно викладені наукові завдання дослідження та шляхи їх вирішення. З тексту зрозуміла наукова і практична значущість роботи, особистий внесок здобувача.

Дискусійні положення та зауваження щодо дисертаційного дослідження.

1) Мета роботи сформульована некоректно. Виходячи з наданих матеріалів метою дисертаційного дослідження має бути, наприклад, підвищення живучості ІС в умовах впливу кібератак за рахунок мінімізації ризиків безпеки таких систем.

2) При формулюванні другого наукового завдання (стор.3 автореферату та стор. 22 дисертації) авторові бажано було б застосовувати суто математичну термінологію: не «механізм», а, наприклад «процедура».

3) До основного змісту дисертаційної роботи, розкритого на 360 аркушах, автором помилково включено сторінки з таблицями та рисунками, які повністю займають площу сторінки, що є неприпустимим. Виходячи з такого обсяг основного змісту роботи становитиме не більше 312 аркушів.

4) В першому розділі дисертаційної роботи авторові було б доцільно:

- більш детально розглянути та описати результати аналізу широкого спектру існуючих засобів та методів аналізу та оцінювання ризиків безпеки ІС;
- провести порівняння відповідних існуючих засобів і розроблених авторських систем оцінювання ризиків відносно застосованих множин параметрів.

5) В четвертому розділі дисертаційного дослідження (п. 4.1) та авторефераті (стор. 17 -21) автором оголошено про:

- використання функції належності, що відображаються лише трапецієвидними нечіткими числами, але не здійснюється обґрунтування їх вибору;
- розроблений метод перетворення інтервалів в нечіткі числа для систем аналізу та оцінювання ризиків ІБ за допомогою трапецієподібних нечітких чисел, але в при математичному описі використано як трапецієподібні, так і трикутні НЧ, що в даному випадку є неприпустимим.

6) В дисертації (стор. 25-26) та авторефераті (стор.5) авторові бажано б було вказати про документальне підтвердження (наприклад актами впровадження) кожної практичної цінності, а не представляти це підтвердження в узагальненому вигляді після їх перерахування. Більший акцент необхідно було б зробити на практичні

цінності починаючи з третього пункту практичного значення отриманих результатів.

Зазначені недоліки не є визначальними. Вони суттєво не впливають на загальне позитивне враження від роботи, не зменшують її наукової цінності та практичної значимості.

3. Відповідність дисертаційної роботи встановленим вимогам та загальний висновок

Дисертаційна робота *КАЗМІРЧУК Світлани Володимирівни* за темою «Методологія оцінювання ризиків безпеки ресурсів інформаційних систем» є завершеною, одноосібно написаною кваліфікаційною науковою працею, що:

1) являє собою системне дослідження, проведене з певною метою;

2) має внутрішню єдність і свідчить про особистий внесок автора в науку;

3) розв'язує актуальну проблему, яка має важливу наукову і практичну спрямованість й результати вирішення якої за рахунок організації системи мінімізації ризиків безпеки ІС істотно впливають на підвищення живучості ІС в умовах впливу кібератак.

За актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною значимістю одержаних результатів дисертаційна робота Казмірчук С.В. відповідає паспорту спеціальності 05.13.21 – «системи захисту інформації», а також вимогам «Порядку присудження наукових ступенів і присвоєння вчених звань старшого наукового співробітника», а її автор *КАЗМІРЧУК Світлана Володимирівна* заслуговує присудження їй наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «системи захисту інформації».

Офіційний опонент
доктор технічних наук, професор, професор кафедри
інформаційних технологій і математичних дисциплін
Факультету інформаційних технологій та управління
Київського університету імені Бориса Грінченка В.Л.Бурячок

ВЛАСНОРУЧНИЙ ПІДПИС
Бурячка В. Л.
ЗАСВІДЧУЮ
(ПІБ)
Мамінько Л.
(підпис)