Прим. № 1

Голові спеціалізованої вченої ради Д 26.062.17
при Національному авіаційному університеті

03058, м. Київ, пр. Космонавта Комарова, 1.

ВІДГУК

офіційного опонента

начальника науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова доктора технічних наук, старшого наукового співробітника Грищука Руслана Валентиновича на дисертацію Гололобова Андрія Юрійовича "Методи та моделі адаптивних систем оцінки ризиків", поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захист інформації

Актуальність теми

В умовах постійного збільшення кількості на нарощування складності кібератак роль систем захисту інформації при забезпеченні безпеки ресурсів інформаційних систем тільки зростає. Ключовою компонентою системи захисту інформації, будь-то антивірусна система, міжмережний екран чи засіб аналізу захищеності, на яку безпосередньо покладаються функції визначення заданого рівня захищеності ресурсу, є підсистема аналізу та оцінювання ризиків. Комплексний характер загроз, їх випадкова природа та різноманітне подання на сьогодні вже суттєво обмежують застосування на практиці систем захисту інформації, підсистеми аналізу та оцінювання ризиків яких функціонують на "класичних" принципах. Тому розроблення нових і удосконалення існуючих методів та моделей оцінювання ризиків безпеки ресурсів інформаційних систем, є актуальною науковою задачею. Зважаючи на зв'язок теми дисертаційного дослідження Гололобова А. Ю. з означеними вище питаннями, її важливість для науки та практики, вважаємо її актуальною.

Оцінка обґрунтованості наукових положень, висновків та рекомендацій сформульованих у дисертації, їх достовірність, новизна

Сформульовані в дисертаційній роботі наукові положення, висновки та рекомендації достатньо повно обґрунтовані здобувачем та викладені в доказовій формі.

Наукова новизна одержаних особисто здобувачем результатів полягає у 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, дозоляє ефективно організовувати процес вибору відповідних існуючих інструментальних засобів і розробляти гнучкі та ефективні методи і систем 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 та нечіткими величинами з варіативним числом терм-множин;

удосконалено модель процесу синтезу систем оцінювання ризиків, яка за рахунок використання базових методів інкрементування та 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 обчислюваних 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, дозволяє формувати і перетворювати дані як в якісній, так і кількісній інтерпретації з можливістю трансформування еталонів параметрів без залучення експертів відповідної області.

Достовірність наукових положень

Достовірність наукових положень дисертаційної роботи підтверджується наступними факторами:

коректна постановка задачі дисертаційного дослідження;

використанням в роботі математично обгрунтованих та широко апробованих на практиці методів теорії нечітких множин та нечіткої логіки, методів теорії прийняття рішень, об'єктно-орієнтованого програмування імітаційного моделювання, методів "м'яких" обчислень.

доброю збіжністю теоретичних розрахунків і результатів імітаційного моделювання (стор. 161 дисерт., стор 15 автореф.);

відповідністю наукових положень основним законам і явищам природи, їх зрозумілим фізичним змістом.

Наукове значення дисертаційної роботи полягає в подальшому удосконаленні методів та моделей оцінювання ризиків безпеки ресурсів інформаційних систем в інтересах створення гнучких засобів оцінювання з адаптивними еталонами параметрів.

Практичне значення дисертаційного дослідження полягає в тім, що здобувачем закладено основи практичного оцінювання ризиків безпеки ресурсів інформаційних систем, які подаються як в числовій так і лінгвістичній формах із застосуванням експертних оцінок, що формуються в слабоформалізованому середовищі.

Одержані здобувачем наукові результати можуть бути використані у науково-дослідних організаціях та підприємствах, що займаються проектуванням та створенням нових систем захисту інформації для оцінювання ризиків безпеки ресурсів інформаційних систем на основі лінгвістичних та цифрових даних.

Практична значимість одержаних результатів і достовірність наукових положень підтверджені актами впровадження, копії яких приведено у дисертації (стор. 180–182) і на які в авторефераті посилається здобувач (стор. 15), що підтверджують про особистий вклад здобувача в науку.

Мова та стиль викладення дисертації та автореферату дозволяють зрозуміти суть розроблених наукових положень та одержаних практичних результатів. Дисертація та автореферат у цілому відповідають вимогам, які висуваються до його оформлення відповідно до "Порядку присудження наукових ступенів" затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами) та суттєво не відхиляються від вимог ДСТУ 3008-2015 "Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення" й "Вимог до оформлення дисертації" затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40.

Поряд з тим є й деякі відхилення від зазначених керівних документів. Наприклад, у дисертаційній роботі на стор. 50 приведено рис. 1.3, а посилання на нього вперше введено на стор. 52.

В цілому зміст дисертації та автореферату викладено послідовно та логічно.

Підтвердження повноти викладу основних результатів дисертації в опублікованих працях

За напрямом дисертаційних досліджень здобувачем опубліковано 15 наукових праць. З них 9 публікацій за темою дисертації в наукових провідних фахових журналах та збірниках наукових праць з технічних наук, 8 з яких належать до рецензованих видань, включених до міжнародних наукометричних баз даних. На міжнародних і регіональних конференціях здобувачем апробовано 6 робіт.

Перелічені публікації з достатньою повнотою відбивають наукові та практичні результати дисертації.

З праць, що їх опубліковано у співавторстві, у дисертації використано лише ті результати, які отримано здобувачем самостійно.

Недоліки

До основних недоліків дисертаційної роботи можна віднести такі.

1. При викладенні матеріалів першого розділу дисертаційної роботи автором приведено досить детальний аналіз загальновідомих понять, наприклад, на стор. 14–17 достатньо детально викладені відомості таких часто вживаних дефініцій, як «інформація» та «інформаційна безпека». На наш погляд було б доцільним лише привести коротке визначення зазначених категорій та вказати посилання на відповідні джерела, у понятійному тлумаченні яких вони уживані в дисертаційній роботі та авторефераті.

Також даний розділ переобтяжений тлумаченням категорії ризик з позиції різних сфер діяльності суспільства та держави. Коректним було б привести у чітку відповідність назву підрозділу 1.2 зі змістом, який викладений у ньому.

2. У дисертації, як і в авторефераті відсутня формалізована постановка наукової задачі дослідження, як це прийнято в галузі технічних наук. Але справедливо слід відмітити й те, що задачі дослідження у дисертації (стор. 9–10) і в авторефераті (стор. 2–3) сформульовано чітко та однозначно

3. На стор. 59 дисертації та стор. 7 автореферату відповідно при розробленні бістабільної інтегрованої кортежної моделі характеристик ризику автор не узагальнює введені ним варіанти адаптивності нечітких шкал оцінювання на конкретний клас нечітких чисел. Ним лише приводяться приклади трапецієвидних та трикутних нечітких чисел.

На наш погляд було б коректним введення обмеження на клас параметричних *AES* нечітких чисел. Такий підхід дозволив би конкретизувати одержані автором результати й відповісти на питання адекватності розробленої моделі у тому разі, якщо в якості параметричних чисел буде використано інші нечіткі числа, крім тих що наведені як приклад.

4. На стор. 62–63 дисертації та стор. 8 автореферату відповідно автор приводить безальтернативне твердження про те, що *«При виникненні труднощів з отриманням статистичних даних або для простоти інтерпретації величин, експерти часто використовують логіко-лінгвістичний підхід»* (див. автореф.). Така безальтернативність призводить до неоднозначного правила відображення характеристики за допомогою лінгвістичної змінної “Імовірність” у разі відсутності статистичних даних.

5. При розробленні методів інкрементування та декрементування (стор. 82 дисертації та стор. 10 автореф. відповідно) автор постулює число термів лінгвістичної змінної для двох найбільш поширеніших типів розподілів нечітких чисел. Таке постулювання ставить під сумнів достовірність розроблених методів у разі зміни типу розподілу нечітких чисел.

Поряд з тим справедливо слід відмітити те, що здобувач доводить достовірність розроблених методів для визначених ним типів розподілів нечітких чисел в четвертому розділі дисертації.

6. Розкриваючи сутність інтегрованого методу аналізу і оцінювання ризиків інформаційної безпеки (стор. 84–93 дисерт. та стор. 10–12 автореф.) складно оцінити які саме аналітичні математичні співвідношення запропоновані особисто автором, а які ним використано з відомих джерел. Наприклад, приводячи оцінку рівня значимості оціночних компонентів посилання на першоджерело [93] приведено, а в інших виразах, наприклад, 3.8 – ні. Якщо це авторська доробка то коректно уживати дієслова доконаного вигляду – співвідношення (математичний вираз) введено, розроблено, запропоновано тощо.

7. Приводячи модель процесу синтезу адаптивних систем оцінювання ризиків безпеки ресурсам інформаційних систем (стор. 93 дисерт. та стор. 12 автореф. відповідно) автор на п'ятому етапі цілком вірно описує множину порушень базових характеристик безпеки відповідною множиною *E*. При цьому на схемі моделі (рис. 3.1 дисерт. та рис. 2 автореф. відповідно) відмічає тільки три базові характеристики – конфіденційність, цілісність та доступність.

Вважається коректним на зазначених схемах введення багатокрапок між цілісністю та доступністю, як це зроблено на інших етапах.

8. Відповідно до вимог, що висуваються до оформлення дисертації в першому пункті висновків слід коротко здійснити оцінку стану питання, що досліджувалося. В дисертації на стор. 164 такий короткий аналіз відсутній, хоча він приведений автором у висновках до автореферату на стор. 17. Також не зроблено акценту на кількісних показниках здобутих результатів.

Вказані недоліки дещо знижують цінність одержаних наукових та практичних результатів, але їх наявність не впливає на загальний позитивний висновок щодо дисертації.

Висновки

Отже, на основі вивчення дисертації, автореферату дисертації та праць здобувача, опублікованих за темою дисертації, **встановлено:**

дисертаційна робота Гололобова А. Ю. відповідає вимогам "Порядку присудження наукових ступенів", затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами);

дисертаційна робота відповідає п. 2 паспорту спеціальності 05.13.21 – системи захисту інформації;

зміст автореферату ідентичний основним положенням дисертації. Але є деякі незначні розходження, обумовлені тим, що автореферат підготовлено на державній мові, а дисертацію – на російській;

дисертація Гололобова А. Ю. є завершеною кваліфікаційною науковою працею, що місить нові науково обгрунтовані результати проведених здобувачем досліджень,

які розв'язують конкретне наукове завдання, що полягає в оцінюванні ризиків безпеки ресурсів інформаційних систем в нечітких та детермінованих умовах з врастанням параметрів, які можуть бути поданими як в числовій., так і лінгвістичній формі із застосуванням експертних оцінок, що формуються у слабоформалізованому середовищі шляхом створення нових та удосконалення існуючих та створення нових методів та моделей. Дане наукове завдання має істотне значення для подальшого розвитку теорії і практики захисту інформації;

автор дисертації ГОЛОЛОБОВ Андрій Юрійович заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Начальник науково-дослідного відділу
інформаційної та кібернетичної безпеки наукового центру
Житомирського військового інституту імені С. П. Корольова

доктор технічних наук,
старший науковий співробітник Р. В. ГРИЩУК

"27" березня 2017 року.

Підпис ГРИЩУКА Р. В. засвідчую.
Начальник відділу особового складу та стройового

О. В. КОВАЛЬЧУК