До спеціалізованої вченої ради Д 26.062.17
Національний авіаційний університет
03058, м. Київ, пр. Космонавта Комарова, 1

ВІДГУК

офіційного опонента
доктора технічних наук, доцента Опірського Івана Романовича
на дисертаційну роботу Корченко Анни Олександрівни
«Методи ідентифікації аномальних станів для систем виявлення вторгнень»,
представлену на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.21 – «Системи захисту інформації»

Актуальність обраної теми. З стрімким розвитком інформаційних технологій зростає кількість уразливостей та загроз ресурсам інформаційних систем і тому для забезпечення їх нормального функціонування та попередження вторгнень необхідні спеціалізовані засоби безпеки. А перспективним напрямком, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в інформаційних системах. Для виявлення мережевих вторгнень використовуються сучасні методи, моделі, засоби і комплексні технічні рішення для систем виявлення та запобігання вторгнень, які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Загалом при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому системи виявлення вторгнень повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні.

Таким чином, дисертаційна робота Корченко Анни Олександрівни, виконання якої направлене на вирішення важливої науково-прикладної

Вх. N 0406/2019
від 20.06.2019 р.

проблеми, пов'язаної з розробкою ефективних методів ідентифікації аномальних станів для систем виявлення вторгнень, є актуальною.

Також актуальність і практичне значення наукового дослідження підтверджується у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету: № 25/09.01.08 «Методи та моделі виявлення уразливостей в ресурсах інформаційних систем» (2015-2017 рр.), № 19/14.01.05 «Системи мультирівневого розмежування доступу до інформаційних ресурсів» (2018-2019 рр.).

Ступінь обґрунтованості та достовірність наукових положень, висновків і рекомендацій, сформульованих у дисертації підтверджується коректною постановкою завдань, науковою обґрунтованістю теоретичних положень, використанням апробованого математичного апарату, узгодженістю теоретичних положень з результатами експериментальних досліджень, опублікованими науковими працями у фахових виданнях та відповідними актами впровадження у діяльність Товариства з обмеженою відповідальністю «Сайфер БІС», а також використовуються в навчальному процесі кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету, кафедри інформаційної безпеки, Інституту інформаційних та телекомунікаційних технологій казахського національного дослідного технічного університета ім. К.І. Сатпаєва і кафедри інформатики та автоматики Технічно-гуманістичної академії у Бельсько-Бялій (Польща).

Наукова новизна результатів роботи. На основі аналізу результатів дослідницької роботи Корченко А.О., можна зробити висновок, що найбільш суттєвими новими науковими результатами, які одержані нею у дисертації, є такі:

•Вперше розроблена кортежна модель формування атакуючих середовищ, яка дозволяє сформувати набір часткових кортежів, за якими здійснюється симуляція процесу виявлення аномального стану в m-вимірному

гетерогенному параметричному середовищі, утвореного відповідним атакуючим середовищем у заданий часовий проміжок.

•Вперше розроблений метод формування еталонного середовища, який дозволяє формалізувати процес отримання еталонних значень фіксованих параметрів заданих груп лінгвістичних змінних, що характеризує конкретне еталонне підсередовище.

•Вперше розроблені методи фазифікації та дефазифікації параметрів, які дозволяють формалізувати процес перетворення значень параметрів *m*-вимірних поточних середовищ для їх подальшого застосування у виявленні аномального стану та відобразити параметри детекційного середоваща, що характеризують у числовій формі рівень упевненості експерта відносно його суджень щодо можливих кібератак.

•Вперше розроблений метод α-рівневої номіналізації нечітких чисел, який дозволяє здійснити графічну інтерпретацію нечітких величин та визначати ідентифікуючі терми, що відображають поточні стани еталонних та поточних підсередовищ, які характерні для реалізації певних типів кібератак на ресурси інформаційних систем.

•Вперше розроблений метод визначення ідентифікуючих термів, який дозволяє за допомогою еталонного середовища здійснити пошук ідентифікуючих перетворених еталонних термів, орієнтованих на обробку в детекційному середовищі для визначення рівней аномальних станів.

•Вперше розроблений метод формування детекційного середовища, який на основі запропонованої кортежної моделі за рахунок механізму формування підмножин ідентифікаторів аномальності, формалізації процесу побудови вирішальних функцій та умовних детекційних виразів, дозволяє сформувати необхідну множину детекційних правил, що використовуються для визначення рівней аномальних станів, характерних впливу певних типів кібератак.

•Вперше розроблена методологія побудови систем виявлення аномалій породжених кібератаками, яка дозволяє будувати системи, що

використовуються для визначення рівня аномального стану в m-вимірному гетерогенному параметричному середовищі.

Теоретичне та практичне значення роботи. Представлені в роботі модель, методи та методологія побудови систем виявлення аномальних станів, породжених реалізацією нових типів загроз, орієнтованої на створення засобів, що розширюють функціональні можливості сучасних систем виявлення вторгнень є важливим теоретичним внеском у наукову спеціальність 05.13.21 – «системи захисту інформації». Практичне значення отриманих результатів полягає у розробленні алгоритмічного та програмного забезпечення модулів, що реалізують побудову еталонних середовищ для систем виявлення кібератак, структурного рішення, алгоритмів та програмної моделі системи для виявлення аномальних станів, породжених кібератаками, яка може використовуватися для розширення функціональні можливості сучасних систем виявлення вторгнень.

Рекомендації щодо використання у дисертації результатів, одержаних автором. Теоретичні та практичні результати дисертаційної роботи доцільно використовувати в організаціях як приватного, так і державного секторів, а також в науково-дослідних та навчальних установах України, які займаються теоретичними та практичними питаннями, пов'язаними з розробленням та аналізуванням ефективності функціонування систем захисту інформації, що обробляється в інформаційних системах. Зокрема, отримані результати можуть бути використані для ефективного вибирання існуючих або розширення функціональні можливості сучасних систем виявлення вторгнень.

Повнота викладення наукових положень дисертації в опублікованих працях. Основні результати за темою дисертації автором викладено в опублікованих 42 наукових працях, які представлені у списку використаних джерел дисертаційної роботи. Зокрема, 3 колективні монографії, 6 наукових статей в міжнародних рецензованих виданнях, що входять в бази даних Scopus та Web of Science (в періодичних та неперіодичних виданнях), 4 наукові статті в іноземних наукових журналах, 19 наукових статей у вітчизняних наукових

журналах, які входять в інші міжнародні наукометричні бази даних, 10 матеріалів та тез доповідей міжнародних конференцій.

За своїм змістом та отриманими результатами дисертаційна робота відповідає формулі та пунктам напрямів досліджень паспорту спеціальності 05.13.21 – «системи захисту інформації», а саме: пункту 1 в частині розроблення «теоретичних, методологічних, технічних <…> основ створення комплексних систем захисту інформації…»; пункту 2 в частині розроблення «… архітектури, методології проектування, технології функціонування систем захисту інформації»; пункту 8 в частині розроблення «моделювання процесів нападу на інформацію та її захисту»; пункту 9 в частині розроблення «методи і засоби вимірювання й обчислення параметрів небезпечних сигналів». Вона є завершеною кваліфікаційною працею з науковими положеннями, що надані автором для публічного захисту, характеризується внутрішньою єдністю та доводить особистий внесок автора в науку.

При цьому зміст автореферату повністю відображає основні положення дисертаційної роботи.

Зауваження до дисертації. Незважаючи на достатній рівень виконаних наукових досліджень до дисертаційної роботи є такі зауваження:

1. Оскільки з аналізу першого розділу прослідковується недосконаліть і неготовність сучасних систем виявлення вторгнень адаптовуватися в реальному часі до виявлення аномалій, породжених модифікованими чи невідомими атаками, то автору доцільніше було б більш ширше розглянути такі методи виявлення вторгнень, які використовують методи нечітких множин.

2. У другому розділі при розробці методу формування еталонного середовища для формального відображення суджень експерта, що характеризує поточний стан параметрів відносно кібератаки, було б доцільно врахувати такі чинники, як узгодженість суджень експертів та рівень їх компетентності.

3. В дисертаційному досліджені всі методи орієнтовані на обробку еталонних та поточних значень непараметричних дискретних нечітких чисел, але не розглянуто як можна застосувати запропоновані методи для обробки інших типів НЧ, наприклад, трапецієподібних та трикутних.

4. Дисертація має обсяг основного тексту 309 сторінок, а також велику кількість об'ємних формул, частина яких займає декілька сторінок, що робить роботу досить великою та складною для сприйняття. Деякі малюнки в авторефераті та дисертації є важкими для сприйняття через їхній розмір та нагромадження.

5. В дисертаційній роботі та авторефераті не здійснюється порівняння технічних показників запропонованих розробок з існуючими системами виявлення вторгнень.

6. В дисертацій роботі методи, що використовуються для побудови еталонів більше орієнтовані на ручний режим, що потребує значного об'єму часу для налаштування розробленої системи.

7. При формуванні наукової новизни, практичної цінності та висновків автор наголошує на розробленні великої низки нових методів, методології та програмного забезпечення, проте у авторефераті і дисертаційній роботі не зазначає про наявність патентів на корисну модель, винахід чи промисловий зразок. Наявність патентів на отримані автором наукові та практичні результати підвищили б вагомість роботи та ступінь її новизни.

Висновки. Зазначені у відгуку зауваження не зменшують теоретичної та практичної цінності дисертаційної роботи Корченко Анни Олександрівни. Загалом, вона характеризується внутрішньою єдністю, виконана на належному науковому рівні та є завершеною працею. В ній отримано нові науково обґрунтовані результати, що в сукупності вирішують науково-прикладну проблему, пов'язану з виявленням нових видів кібератак за максимально короткий час за допомогою відповідної методології побудови систем виявлення аномальних станів, породжених реалізацією нових типів загроз,

орієнтованої на створення засобів, що розширюють функціональні можливості сучасних систем виявлення вторгнень.

За актуальністю науковою новизною, практичною значущістю та сформульованими науковими положеннями вважаю, що дисертаційна робота Корченко Анни Олександрівни «Методи ідентифікації аномальних станів для систем виявлення вторгнень» відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 № 567, а її автор заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент,
доцент кафедри захисту інформації
Національного університету
«Львівська політехніка»
доктор технічних наук, доцент І.Р. Опірський

Підпис доцента Опірського І.Р. засвідчую
Вчений секретар Національного університету
«Львівська політехніка», к.т.н., доцент Брилинський Р.Б.