Голові спеціалізованої вченої ради Д 26.062.17
при Національному авіаційному університеті
03058, м. Київ, просп. Космонавта Комарова, 1

ВІДГУК
офіційного опонента

начальника кафедри захисту інформації та кібербезпеки Житомирського військового інституту імені С. П. Корольова доктора технічних наук, професора Грищука Руслана Валентиновича на дисертацію Корченко Анни Олександрівни "Методи ідентифікації аномальних станів для системи виявлення вторгнень", поданої нею на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації

Актуальність теми

Інформаційні системи та інформаційні технології, які покладені в їх основу, відіграють на сьогодні визначальну роль у процесі створення, накопичення, зберігання, передавання та розповсюдження інформаційних ресурсів. Цінність таких інформаційних ресурсів, залежно від їх критичності, варіює. Наприклад, цінність ресурсів інформаційних систем (ІС), що становлять державну таємницю тобто державних інформаційних ресурсів може бути співвимірною зі збитками, які матимуть місце у разі доступу до них неавторизованих користувачів. У нинішній ситуації в нашій державі наслідки взагалі можуть мати катастрофічний характер для економіки, фінансового сектору, сфери безпеки і оборони тощо.

Нині світова та національна практика забезпечення захищеності ІС зводиться до застосування в інформаційних системах трьох основних типів систем захисту інформації, а саме міжмережних екранів, антивірусних засобів та засобів аналізу захищеності. На наш погляд та погляд інших фахівців з інформаційної й кібернетичної безпеки найбільш перспективними на сьогодні є саме засоби аналізу захищеності. Найбільш розповсюдженими з них, які відомо, є такі, як системи виявлення атак та системи виявлення вторгнень (СВВ), останні з яких з причини потенційної можливості забезпечення проактивного захисту становлять особливий практичний інтерес. Таким чином, СВВ є перспективним класом систем захисту інформації удосконалення та розвиток яких є пріоритетним напрямом наукових досліджень багатьох університетів та дослідницьких установ світу.

Не зважаючи на значну кількість досліджень у згаданій царині на сьогодні й досі існувало об'єктивне протиріччя між постійно зростаючими витратами на оперативний моніторинг та блокуванням нових видів кібератак та неухильним зростанням збитків власників ІС, що обумовлені високою інерційністю існуючих СВВ до нових типів кіберзагроз. Тому розвиток методів ідентифікації аномальних станів, що усувають визначене протиріччя в СВВ, є актуальною науковою проблемою. *Отже, зважаючи*

на зв'язок теми дисертації Корченко А. О. з означеними вище питаннями, вважаємо її достатньо обґрунтованою та актуальною.

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

Загальна характеристика дисертації

У **вступі** здобувачем подано загальну характеристику роботи, обґрунтовано актуальність обраної теми, сформульовано мету і завдання дослідження, відображено наукову новизну й практичну цінність одержаних результатів, наведено дані щодо їх апробації та впровадження.

У **першому розділі** здобувачем приведено результати аналізу сучасних систем виявлення вторгнень. Зокрема при проведенні аналізу базових характеристик систем виявлення вторгнень *здобувачкою встановлено*, що у відкритих джерелах відсутній опис необхідної множини характеристик для інтегрованої оцінки СВВ при їх практичній реалізації. *Показано*, що наявні характеристики, які названо базовими, можуть бути використані лише для вибору з усієї множини доступних СВВ тих, які здатні на програмному та (або) апаратно-програмному рівні ідентифікувати кібератаки.

Позитивною рисою першого розділу є те, що в ньому приведено результати ґрунтовного науково-технічного аналізу усіх сучасних та наявних у відкритому доступі СВВ. Питання аналізу торкнулися дослідження не тільки інтерфейсної частини СВВ, а й функціональної. *Як результат одержано* зведені дані по відкритим СВВ, що виступають підґрунтям для подальшого їх розвитку та удосконалення. Також у першому розділі *систематизовано та проаналізовано* програмні та програмно-апаратні засоби виявлення вторгнень. *Таким чином, одержані здобувачкою у першому розділі результати виступили науковим підґрунтям для постановки проблеми в загальному вигляді та формалізації на її основі частинних наукових завдань, які також приведені у розділі.*

У **другому розділі** приведено розроблені методи формування еталонного середовища для ідентифікації аномальних станів. З метою зняття невизначеності в частині, що стосується уживаних дефініцій *здобувачкою запропоновано власну термінологію* уживаних у дисертації термінів та понять. Так, зокрема, введено терміни "аномальний стан", "атакуюче середовище" тощо. В основу моделі формування атакуючих середовищ здобувачем покладено розроблену у розділі кортежну модель. В умовах гетерогенного середовища це безумовно *є перевагою* запропонованої моделі, оскільки такий підхід дозволив формалізувати власне атакуюче середовище. Запропонована кортежна модель досить легко сприймається фахівцями, оскільки при розкритті компонент кортежу здобувачкою наводяться конкретні частинні випадки, а також вигляд якого набуває модель для тих чи інших характеристик m- вимірного атакуючого гетерогенного середовища, утвореного відповідним атакуючим середовищем у заданий часовий проміжок.

Для практичної реалізації кортежної моделі у розділі *приведено розроблений особисто здобувачкою* метод формування еталонного середовища. Зокрема *перевагою* розробленого методу є те, що він дозволяє формалізувати процес отримання еталонних значень фіксованих параметрів визначених груп лінгвістичних змінних. Далі у розділі приводяться по-суті модифікації даного методу для найбільш небезпечних типів кібератак та способів їх реалізації, зокрема таких, як сніфінгу та e-mail- спуфінгу. На наш погляд використання в якості вхідних даних результатів моделювання у віртуальному середовищі вказаних типів кібератак суттєво підкріплює достовірність розроблених методів. *Таким чином, розроблені в другому розділі методи є теоретичним підґрунтям для ідентифікації аномальних станів СВВ.*

Третій розділ дисертації здобувачка присвятила розробленню базових методів формування поточного середовища. Зокрема *розроблено метод* фазицікації параметрів на еталонних підсередовищах для систем виявлення кібератак, *метод α- рівневої номіналізації нечітких чисел* та *метод визначення ідентифікуючих термів* для СВВ. Так *підтвердженням достовірності методу фазицікації параметрів на еталонних підсередовищах є* використання в якості вхідних даних параметрів підключення веб-сервера визначеної конфігурації, посилання на який приведено у списку літератури до розділу. Але, слід відмітити, що не вказання параметрів такого веб-сервера *є дещо некоректним* до стилю викладення одержаних результатів, чим самим потребує пошуку відповідного першоджерела. При викладенні методу *α- рівневої номіналізації нечітких чисел* здобувачка зазначила та аргументовано довела, що для СВВ даний метод дозволяє здійснювати графічну інтерпретацію нечітких величин та визначати ідентифікуючі терми, що відображають поточні стани еталонних та поточних підсередовищ, які характерні для реалізації певних типів кібератак. *Третій метод*, який розроблено в даному розділі ґрунтується на перших двох методах та за допомогою еталонного середовища дозволяє здійснити пошук ідентифікуючих перетворених еталонних термів, орієнтованих на оброблення в детекційному середовищі для визначення рівнів аномальних станів. *Таким чином, одержані у третьому розділі наукові результати є базовим підґрунтям для створення нового класу СВВ.*

У **четвертому розділі** здобувачкою розроблено методи виявлення аномальних станів породжених кібератаками. Зокрема при розробленні методу дефазифікації параметрів детекційного середовища *обґрунтовано* етапи, які складають його зміст. На наш погляд, з практичної точки зору, становить інтерес третій, заключний, етап методу. Такий підхід, на відміну від відомих, дозволяє залучати експертні знання до виявлення аномальних станів, породжених кібератаками. *Особливістю* розробленого та поданого у даному розділі методу формування детекційного середовища для СВВ є формування підмножини ідентифікаторів аномальності, що на відміну від відомих підходів, які ґрунтуються на стандартних функціональних профілях захищеності є новим. По суті даний метод вирішує зворотну безпекову задачу – не з позиції те, що потрібно захищати в інформаційній системі, а те, від чого слід захищатися.

На заключення, у четвертому розділі, здобувачкою розроблено *методологію* побудови систем виявлення аномалій, породжених кібератаками. Запропонована

методологія є науково обґрунтованою та такою, що має важливе практичне застосування. Так у практичному плані розроблена методологія дає відповідь на такі питання, як слід будувати сучасні СВВ на які покладаються завдання з виявлення аномалій в інформаційних системах різного цільового призначення в складних багатовимірних гетерогенних середовищах. Таке подання одержаних результатів без сумніву можна вважати перевагою даного дослідження.

П'ятий розділ є заключним. У даному розділі *запропоновано* структурну та алгоритмічну реалізацію розроблених у попередніх розділах методів та методології, а також приведено результати верифікації програмного модуля системи виявлення кібератак.

Запропоноване структурне рішення побудови системи виявлення кібератак суттєво нарощує функціональні можливості відомих СВВ. Так, наприклад, функціональні можливості сучасних СВВ нарощено в частині, що стосується визначення рівня аномального стану, а також характерного впливу певного типу кібератак в слабоформалізованому нечіткому середовищі оточення. Здобувачкою у п'ятому розділі також *розроблено програмне забезпечення*, яке використано для перевірки роботоспроможності запропонованих методів та методології. Працездатність даного програмного забезпечення *підтверджується* використанням в якості функціональної основи базового алгоритму *System_level_Click* з відповідними зумовленими процесами (процедурами). Верифікацію програмного модуля системи виявлення кібератак здійснено у спеціально сконфігурованій для цього віртуальній мережі, що додатково підкреслює практичну цінність одержаних в дисертації наукових результатів. Таким чином, усі *наукові результати одержані у попередніх розділах підтверджено* практично або за результатами моделювання, або за результатами верифікації.

У **висновках** приведено основні одержані результати, їх наукову та практичну цінність. Подано дані щодо впровадження результатів роботи, основні рекомендації та дані щодо їх впровадження.

У **додатках** до дисертації наведено: копії актів реалізації; програмні коди модулів системи виявлення кібератак; стани поточного *SP*- середовища, що відображаються вихідними масивами даних.

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

Наукова новизна одержаних особисто здобувачкою результатів полягає у такому.

– *вперше* розроблено кортежну модель формування атакуючих середовищ, яка за рахунок формалізації процесу створення m_i - вимірних параметричних, атакуючих, еталонних, поточних та детекційних підсередовищ, 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* розроблено метод формування еталонного середовища, який за рахунок використання множини ідентифікаторів лінгвістичних оцінок та ідентифікаторів

інтервалів, базової та похідної матриці частот, формального відображення суджень експерта для характеристики поточного стану параметрів відносно кібератаки, процесу формування на заданих інтервалах частот зустрічальності експертних оцінок та підмножин нечітких термів, дозволяє формалізувати процес отримання еталонних значень фіксованих параметрів заданих груп лінгвістичних змінних, що характеризує конкретне еталонне підсередовище;

– *вперше* розроблено методи фазифікації та дефазифікації параметрів, які на основі еталонних підсередовищ, поправкових і лінгвістичних еталонів підмножин інтервалів для формування частот зустрічальності значень фізичних параметрів в задані моменти очікуваної події та процедури визначення допоміжного терма, експертних коефіцієнтів параметрів і кібератаки, що характеризують експертні лінгвістичні оцінки, пов'язані з рівнем аномального стану в поточному середовищі дозволяють формалізувати процес перетворення значень параметрів m- вимірних поточних середовищ для їх подальшого застосування у виявленні аномального стану та відобразити параметри детекційного середовища, що характеризують у числовій формі рівень упевненості експерта відносно його суджень щодо можливих кібератак;

– *вперше* розроблено метод α - рівневої номіналізації нечітких чисел, який за рахунок побудованого механізму формування множини α-рівнів, допоміжних підмножин α - рівневих інтервалів та міжточкових α - рівневих інтервалів, а також процесу номіналізації та визначення значень необхідних супортів нечітких чисел еталонних та поточних середовищ, 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 за рахунок базового механізму, що реалізує формування елементів множини характерних ознак та використання узгодженої функції, дозволяє за допомогою еталонного середовища здійснити пошук ідентифікуючих перетворених еталонних термів, орієнтованих на обробку в детекційному середовищі для визначення рівнів 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 рівнів аномальних станів, характерних впливу певних типів кібератак;

– *вперше* розроблена методологія побудови систем виявлення аномалій породжених кібератаками, яка за рахунок механізмів формування атакуючих середовищ, побудови m_i - вимірних параметричних еталонних та поточних підсередовищ, α - рівневої номіналізації еталонних та поточних підсередовищ, процесу дефазифікації та визначення ідентифікуючих термів та формування детекційних середовищ дозволяє будувати системи, що використовуються для

визначення рівня аномального стану в m- вимірному гетерогенному параметричному середовищі;

– *вперше* розроблено структурне рішення обчислювальної системи виявлення кібератак, яке за рахунок баз даних кібератак, правил та еталонів, а також модулів формування поточних значень, α - рівневої номіналізації, дефазифікації та ідентифікуючих термів, рівня аномальності та візуалізації дозволяє будувати засоби, які визначають рівні аномального стану, що характерні впливу певного типу кібератак і розширюють функціональні можливості сучасних систем виявлення вторгнень.

Достовірність наукових положень

Достовірність наукових положень дисертаційної роботи підтверджується:

– коректною постановкою наукової проблеми та часткових наукових завдань дисертаційного дослідження (с. 79–81 дисерт. та с. 2, с. 3 автореф.);

– використанням в роботі теоретично обґрунтованих та широко апробованих на практиці методів теорії захисту інформації, системного аналізу, методів теорії множин та теорії нечітких множин, методів та елементів нечіткої логіки, методів прийняття рішень, моделювання та експертного оцінювання, методів аналітичної геометрії та м'яких обчислень, методів теорії алгоритмів, експерименту, об'єктно-орієнтоване програмування, а також імітаційне моделювання інформаційних процесів і структур;

– збіжністю результатів моделювання та експериментальних перевірок з відомими експериментальними даними інших академічних досліджень, відповідністю отриманих теоретичних результатів з результатами експерименту (с. 364, 365 дисерт., с. 30, 31 автореф.);

– відповідністю наукових положень основним законам і явищам природи.

Наукове значення дисертаційної роботи полягає в подальшому розвитку теорії захисту інформації в частині, що стосується створення методів ідентифікації аномальних станів для систем виявлення вторгнень, спроможних виявляти такі стани як для відомих, так і нових типів кіберзагроз.

Практичне значення дисертації полягає в створенні діючого алгоритмічного та програмного забезпечення модулів, що реалізують побудову еталонних середовищ для систем виявлення кібератак, створення нових структурних рішень та програмних моделей для виявлення аномальних станів, породжених кібератаками.

Практична значущість одержаних результатів і достовірність наукових положень підтверджені актами впровадження, копії яких наведено у дисертації (с. 374–377) і про що зазначено в авторефераті на с. 5, що підтверджують особистий внесок здобувача в науку.

Мова та стиль викладення дисертації та автореферату дозволяють зрозуміти суть розроблених наукових положень і одержаних практичних результатів. Дисертація і 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 Вимог до оформлення дисертації, затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40. Зміст дисертації та автореферату викладено послідовно та логічно.

Підтвердження повноти викладу основних результатів дисертації в опублікованих працях

За напрямом дисертаційного дослідження здобувачем опубліковано 57 наукових праць. У тому числі: 3 колективні монографії, 6 наукових статей в міжнародних рецензованих виданнях, що входять в бази даних *Scopus* та *Web of Science*, 4 наукові статті в іноземних наукових журналах, 19 наукових статей у вітчизняних наукових журналах, які входять до інших міжнародних наукометричних баз даних, 10 матеріалів та тез доповідей міжнародних конференцій.

Перераховані 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.

Зауваження щодо змісту дисертації та її оформлення

До основних недоліків дисертаційної роботи можна віднести такі.

1. Здобувачкою у першому розділі при проведенні аналізу сучасних систем виявлення вторгнень одержані результати подаються окремо для відкритих систем та програмних й програмно-апаратних систем виявлення вторгнень. На наш погляд такий поділ за визначеними класифікаційними ознаками не досить раціональний, оскільки і відкриті системи виявлення вторгнень, і програмні та програмно-апаратні системи виявлення вторгнень можуть бути одночасно і відкритими, і програмними та (або) програмно-апаратними.

З іншого боку справедливо слід відмітити те, що при узагальненні результатів систем виявлення вторгнень (с. 78–80 дисерт. та с. 6, с. 7 автореф, відповідно) здобувачка прийшла до вірного висновку щодо потреби перегляду класифікаційних ознак обравши такі, наприклад, як *"клас кібератак"*, *"відкритість"*, *"методи виявлення"* та ін.

2. У другому розділі при формалізації підходу до формування базових компонент на основі якого за визначені проміжки часу в слабоформалізованому нечітко визначеному середовищі пропонується виявляти аномальні стани, здобувачкою вводиться ряд нових дефініцій. Наприклад, *"аномальний стан"*, *"атакуюче середовище"*, *"детекційне середовище"*, *"еталонне середовище"* тощо (с. 99, с. 100 дисерт., с. 7 автореф, відповідно), які далі уживаються по тексту дисертації. У цілому з цим можна погодитися. Але при введенні нових термінів і понять в усталеній галузі науки, такій як захист інформації та інформаційна безпека, вважається за доцільне визначення їх місця в уже існуючій дефініційній системі або категорійному апараті, що дозволить визначити зв'язки між тим, що вже існує та тим, що пропонується.

3. При висвітленні процедури опитування експерта щодо стану спостережуваних ним фактичних значень різних параметрів у m - вимірному гетерогенному параметричному середовищі P (с. 127 дисерт., с. 8, с. 9 відповідно) здобувачка не акцентує увагу на ряді важливих на наш погляд питань, які обов'язково мають бути визначені при використанні методів експертного оцінювання. Це стосується, власне,

так званих характеристик самого експерта – його компетенції, кваліфікації, ступеня конформізму тощо, кількості експертів, що залучаються для опитування, методу узгодження експертних оцінок, опитувальних таблиць.

Вважаємо це питання принциповим, оскільки оброблення даних процедури експертного оцінювання суттєво впливатиме на наближеність створюваного m-вимірного гетерогенного параметричного середовища P тому середовищу, в якому відбуваються реальні явища та процеси, пов'язані з аномаліями в інформаційних системах.

4. На наш погляд, здобувачка дещо вільно оперує такими класами систем захисту інформації, як системи виявлення атак (*Intrusion Prevention System (IPS)*) та системи виявлення вторгнень (*Intrusion Detection System (IDS)*). Наприклад, у першому розділі дисертації й автореферату мова йде про системи виявлення вторгнень, а в п'ятому (п. 5.1 та далі за текстом) мова вже йде про системи виявлення кібератак. Звичайно, що дані класи систем захисту відносяться до одного типу, а саме до засобів аналізу захищеності. Але головне те, що дані системи захисту виконують хоч і спорідненні, але все ж таки різні функції. Тому виходячи з функціоналу досліджуваних у п'ятому розділі дисертації систем складається враження, що мова все таки йде про системи виявлення вторгнень, які названі системами виявлення кібератак. Очевидно, що неточність у формулюванні здобувачкою ужита з метою акцентування уваги саме на тому, що створюваний клас систем захисту є новим та таким, який спроможний виявляти аномальну поведінку в складному неформалізованому нечіткому гетерогенному середовищі.

5. Досить вдалим вважаємо використання реальних згенерованих даних для формування частот зустрічальних параметрів за допомогою утиліти *netstat*. Але цього на наш погляд не достатньо, про що, до речі, й сама зазначає здобувачка на с. 212 дисертації. Для зняття невизначеності щодо заповнення таблиці 3.2 з фізичними параметрами, які не генеруються *netstat*, наприклад по кібератакам типу *DOS*, доцільно було б в додаток привести скріни тих *log*-файлів, які аналізувалися. Зазначене дозволило б підкріпити вказані параметри реальними даними, й зняти питання достовірності вхідних даних.

6. Не викликає сумніву факт того, що розроблений особисто здобувачкою метод α-рівневої номіналізації нечітких чисел спроможний здійснювати графічну інтерпретацію нечітких величин та визначати ідентифікуючі терми, що відображають поточні стани еталонних та поточних підсередовищ, які характерні для певних типів кібератак на ресурси інформаційних систем. Даний факт у доказовій формі викладено у третьому розділі. Але без введення обмежень на тип кібератак запропонований метод може розцінюватися як універсальний інструмент, доведення якого до конкретного програмного або програмно-апаратного рішення стане панацеєю від усіх відомих і невідомих кіберзагроз, а це, очевидно, не так. Тому слід бути більш коректним у безапеляційному формулюванні висновків.

7. На наш погляд запропонована у п'ятому розділі (с. 316 дисерт. та с. 27 автоерф., відповідно) структурна схема системи виявлення кібератак (рис. 5.1)

досить повно описує усі необхідні складові типової системи захисту інформації. Схема виглядала б більш виграшно, як що б здобувачка виокремила на ній ті компоненти, які відповідають за запропоновані середовища, наприклад еталонне, атакуюче тощо.

8. У дисертації не знайшло місця питання оцінки помилок першого та другого роду, які є ключовими характеристиками якості функціонування розроблюваних систем виявлення вторгнень. Наявні відсоткові оцінки виявлених кібератак хоч і приведені на с. 365 (с. 31 автореф. відповідно), але вони повинні розглядатися, як доповнення до загаданих вище.

9. У п'ятому розділі здобувачка стверджує, що провела експериментальне дослідження для підтвердження достовірності отриманих теоретичних положень та практичних результатів. Так, дійсно. Такі дані приведені. Вони достовірні. Усі одержані результати описані й проаналізовані. Але на наш погляд не в повній мірі дотримано процедурне питання при проведенні експерименту. Мають бути визначені його назва, мета, завдання, план проведення експерименту, спосіб оброблення результатів тощо.

10. Зважаючи на достатньо обмежений обсяг автореферату, визначений керівними документами, у дисертації хотілося б побачити не тільки виконання формальних вимог стосовно формулювання висновків по розділам та роботі у цілому, а й більш ширше висвітлення одержаних результатів. Наприклад, здобувачка нічого не каже про те, що нею особисто запропоновано новий підхід до побудови проактивних інтелектуальних систем захисту інформації, які спроможні виявляти найнебезпечнішу кіберзагрозу сьогодення, яка проявляється у вигляді кібератаки *0-дня* та ін. Від цього без сумніву робота набула б ще більшого наукового та практичного значення.

Зазначені недоліки дещо впливають на якість подання дисертації, але їх наявність не знижує практичної, а тим паче наукової цінності одержаних здобувачкою результатів.

Висновки

Отже, на основі критичного вивчення дисертації, автореферату дисертації та праць здобувачки, опублікованих за темою дисертації, об'єктивно **встановлено:**

– дисертаційна робота Корченко А. О. відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами);

– дисертаційна робота відповідає п. 1 та п. 2 паспорту спеціальності 05.13.21 – системи захисту інформації;

– зміст автореферату ідентичний основним положенням дисертації;

– результати наукових досліджень, за якими здобувач захистила кандидатську дисертацію, на захист докторської дисертації не виносяться;

– використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувача в науку;

– дисертація Корченко А. О. є завершеною кваліфікаційною науковою працею, що місить нові науково обґрунтовані результати проведених здобувачем досліджень,

які вирішують конкретну науково-прикладну проблему, пов'язану з розробленням ефективних методів ідентифікації аномальних станів для систем виявлення вторгнень. Дана науково-прикладна проблема має істотне значення для подальшого розвитку теорії захисту інформації і створення нових класів систем захисту інформації;

– автор дисертації, КОРЧЕНКО Анна Олександрівна заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент –
начальник кафедри захисту інформації та кібербезпеки
Житомирського військового інституту імені С. П. Корольова

доктор технічних наук, професор Р. В. ГРИЩУК

"05" червня 2019 р.

Підпис професора ГРИЩУКА Р. В. засвідчую.
ТВО начальника відділу персоналу та стройового
В. Ю. КІСЕЛЬОВ